MASTER'S THESIS

# Master of Science in Advanced Mathematics and Mathematical Engineering

**Title:** Iwasawa Theory

**Author:** Pol Torrent i Soler

**Advisor:** Francesc Fité Naya

**Department:** Mathematics

**Academic year:** 2017-18



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master's degree thesis

# Iwasawa Theory

Pol Torrent i Soler

Advisor: Francesc Fité Naya

Department of Mathematics

# Contents

# Introduction

This thesis is intended to offer a first approximation to classical Iwasawa theory. The goal of classical Iwasawa theory is to study the growth of the class group in towers of cyclotomic fields. The class group is a fundamental invariant of a number field $F$. The class group is a measure of the extent to which unique factorization fails in the ring of integers of $F$. The study of the class groups of cyclotomic fields goes back to Kummer, who already recognized the failure of factorization in the ring of integers of a number field as a major obstruction to finding a complete proof of the general case of Fermat's last theorem.

Although the class group is known to behave quite erratically in towers of field extensions in general, in the particular case of towers of cyclotomic fields it exhibits an astonishing regular pattern. This was shown by Iwasawa [**5**] already in the late 50's in the more general context of a $\mathbb{Z}_p$-extension, establishing the so-called Iwasawa control theorem. In a major paper [**7**], Iwasawa predicted the connection between $\mathbb{Z}_p$-extensions and $p$-adic $L$-functions (Iwasawa's Main Conjecture). This conjecture was proven by Mazur and Wiles [**10**] using advanced methods for the study of the geometry of modular curves. The Iwasawa Main Conjecture was later reproven in the works of Kolyvagin [**8**], Thaine [**17**], and Rubin [**12**] using Euler systems. This proof builds on a theorem of Iwasawa relating the $p$-adic zeta function and cyclotomic local units.

Iwasawa theory has been a fruitful research topic in number theory over the last decades. For instance, Mazur and Greenberg have developed generalizations of Iwasawa theory for elliptic curves and, more generally, for abelian varieties. In 2010, Skinner and Urban [**16**] published a celebrated result that proves the Iwasawa Main Conjecture in a more general setting.

This thesis is structured in five chapters. In the first chapter we introduce some preliminary results and concepts that are not related to Iwasawa theory but that are widely used throughout the thesis: we define what is a valuation and how it behaves under field extensions, and we also define what local uniformizing parameter is.

The first part of the thesis (chapters 2 and 3) is devoted to the proof of Iwasawa's control theorem. In chapter 2, we explore the properties of the power series ring $\Lambda = \mathbb{Z}_p[[T]]$ and we present an structure theorem for $\Lambda$-modules (theorem 2.11). In the third chapter, we define what a $\mathbb{Z}_p$-extension is and we give the proof of Iwasawa's control theorem (theorem 3.8).

In the second part of the thesis (chapters 4 and 5) we present the Iwasawa Main Conjecture and we give a proof of Iwasawa's theorem relating the $p$-adic zeta function with cyclotomic local units. In chapter 4 we interpret Iwasawa's control theorem in terms of the characteristic ideal of a Galois group and introduce the basic notation to state the Iwasawa Main Conjecture (theorem 4.7). We also lay out the proof strategy for the Iwasawa Main Conjecture based in three major results, theorems 4.6 (which states the existence of a $p$-adic analogue of the Riemann zeta function), 4.8 and 4.9. Throughout chapter 5 we develop the theory required to prove theorems 4.6 and 4.8, and we finish this thesis by proving those two theorems. We construct the $p$-adic Riemann zeta function as the image by a Coleman map $\widetilde{\mathcal{L}}$ of the Euler system of cyclotomic units $c(a,b)$. This is a powerful method used in many other contexts.

If this thesis were to be continued, the more natural way to do it would be to introduce Euler systems and to complete the proof of the Iwasawa Main Conjecture by proving theorem 4.9 following the argument of Kolyvagin, Thaine and Rubin.

This thesis has two main references. For the first part (the proof of the Iwasawa control theorem) we follow Washington's book [**18**, §13]. For the second one, concerning the Iwasawa Main Conjecture, our main reference is the book by Coates and Sujatha [**2**]. While we do not present any original results, the contribution of this thesis is to join the theory developed in those two references while mantaining a coherent notation and structure. By doing that, we present a comprehensive introduction to classical Iwasawa theory that uses the results from [**18**] to motivate the treatment of the Iwasawa Main Conjecture carried out in [**2**].

Prerequisites. We assume that the reader is familiar with the basic notions usually presented in first courses of algebraic number theory and commutative algebra. We also borrow from Class Field Theory the notion of Hilbert class field as well as a description of the Galois group of a certain field extension in terms of local units modulo global units of a fixed $\mathbb{Z}_p$-extension. We also assume that the reader is familiar with the basic properties of the (complex) Riemann zeta function. Besides from this, the thesis is essentially self-contained.

Notation. We now fix some notation that will be used throughout this thesis:

| | |
|---|---|
| $p$ | denotes an *odd* prime; |
| $\zeta_n$ | denotes a $p^{n+1}$-th root of unity; |
| $\mu_{p^{n+1}}$ | denotes the group of $p^{n+1}$-th roots of unity; |
| $\cup_{n\geq 0}\,\mu_{p^{n+1}} = \mu_{p^\infty}$ | denotes the group of all $p$-power roots of unity. |

The roots of unity considered above are seen as elements of $\overline{\mathbb{Q}}$. However, throughout we will consider a fixed embedding $\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}_p}$ so we will see them as elements of $\overline{\mathbb{Q}_p}$ via that fixed embedding when required.

Acknowledgements. I would like to express my utmost gratitude to my advisor, Francesc Fité, for the countless hours he has devoted to this thesis, for his unlimited patience and for making the experience of writing this thesis one of the greatest experiences I had in my academic life. I would also like to thank my colleague and friend Óscar Rivero for encouraging to choose this thesis, for the many useful discussions we had about it and for all the support he has provided me whenever necessary.

# Chapter 1
# Preliminary results

The aim of this chapter is to introduce some concepts and results for which no background in Iwasawa theory is needed but that will be extensively used in this thesis. We will define the concepts of valuation, valuation ring and uniformizing parameter, and we will see how they behave under field extensions. The reference that we followed for these results is [**11**].

## 1. Non-archimedean valuations

DEFINITION 1.1 (Multiplicative valuation). *A* multiplicative valuation *on a field $K$ is a function $x \mapsto |x| : K \to \mathbb{R}$ such that*

*(1)* $|x| \geq 0$ *and* $|x| = 0$ *if and only if* $x = 0$.
*(2)* $|xy| = |x||y|$ *for all* $x, y \in K$.
*(3)* $|x+y| \leq |x|+|y|$ *(triangle inequality). If the stronger condition* $|x+y| \leq \max\{|x|, |y|\}$ *holds then we say that* $|\cdot|$ *is a* non-archimedean valuation.

Given a multiplicative valuation $|\cdot|$, we will say that the function

$$\begin{array}{rccc} v: & K^\times & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & v(x) = -\log|x| \end{array}$$

is an *additive valuation*, where we used $K^\times$ for the multiplicative group of the field $K$. We say that such a valuation is *discrete* if, and only if $v(K^\times) \subseteq \mathbb{R}$ is a discrete subgroup.

Given a non-archimedean valuation $|\cdot|$, we will call

$$A = \{a \in K \mid \ |a| \leq 1\}$$

the *ring of integers* of $K$. $A$ is what we will call a *valuation ring*, and its units are

$$A^\times = \{a \ \in K \mid |a| = 1\}.$$

$A$ has a unique maximal ideal

$$\mathfrak{M} = \{a \in K \mid |a| < 1\}$$

and it is thus a local ring. It is also easy to check that $\mathfrak{M}$ is principal if, and only if, the valuation is discrete. When that happens, we will say that $A$ is a *discrete valuation ring* (DVR).

The concept of a local uniformizing parameter will be very important to us:

DEFINITION 1.2 (Local uniformizing parameter). *Let $|\cdot|$ be a discrete non-archimedean valuation. A* local uniformizing parameter *$\pi$ is an element of $K$ such that $|\pi|$ has the largest value $< 1$.*

Notice that the local uniformizing parameter is well-defined, as $|K^\times|$ is discrete in a neighbourhood of 1. Equivalently, $\pi$ is the element of $K$ with lowest positive additive valuation $v(\pi)$. One can also see that a local uniformizing parameter is a generator of the maximal ideal $\mathfrak{M}$. We say that an additive valuation $v$ of $K$ is *normalized* if $v(\pi) = 1$, where $\pi$ is a uniformizing parameter of $K$.

We can also note that a multiplicative valuation $|\cdot|$ on a field $K$ endows it with the structure of metric space. In particular, we have the notion of completeness.

## 2. Non-archimedean valuations in field extensions

In this section we explore how non-archimedean valuations work in finite field extensions. Let us fix some notations that we will use for the rest of the section. $K$ will denote a complete field with respect to a non-archimedean valuation $|\cdot|_K$, and let $L/K$ be a finite and separable extension. We have the following result

THEOREM 1.3. *The valuation $|\cdot|_K$ extends uniquely to a discrete valuation $|\cdot|_L$ on $L$.*

*Proof.* Let $A$ be the discrete valuation ring of $K$, and let $B$ be its integral closure in $L$. Let $\mathfrak{p}$ be the maximal ideal of $A$. Since both $A$ and $B$ are Dedekind domains, the valuations of $L$ extending $|\cdot|_\mathfrak{p}$ correspond to ideals in $B$ that are over $\mathfrak{p}$.
We now claim that there is only one prime ideal over $\mathfrak{p}$, which would imply the uniqueness of the extension.
Assume there are two distinct prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ in $B$ that divide $\mathfrak{p}$. If that happens, there is a $\beta \in B$ such that $\mathfrak{P}_1 \cap A[\beta] \neq \mathfrak{P}_2 \cap A[\beta]$ (for instance, take $\beta \in \mathfrak{P}_1, \beta \notin \mathfrak{P}_2$). Let $f(X)$ be the minimal polynomial of $\beta$ over $K$, so that $A[\beta] \cong A[X]/(f(X))$. Since $f(X)$ is irreducible in $A[X]$ and $A$ is complete, we can apply Hensel's lemma to get that $\tilde{f}(X)$ (which is the image of $f$ in $k[X]$ where $k = A/\mathfrak{p}$) must be a power of an irreducible polynomial. Thus

$$A[\beta]/\mathfrak{p}A[\beta] \cong k[X]/(\tilde{f}(X))$$

is a local ring, contradicting the fact that $A[\beta]$ had two distinct prime ideals containing $\mathfrak{p}$. □

Now we will see how the valuation of the uniformizing parameters of the field $L$ is related to the so-called ramification index of the extension $L/K$. We will denote by $A$ and $B$ the integer rings of $K$ and $L$, respectively. Both $A$ and $B$ are local rings. Let $\mathfrak{p} = (\pi)$ be the

maximal ideal of $A$ and $\mathfrak{P} = (\Pi)$ be the maximal ideal of $B$, with $\pi$ and $\Pi$ being uniformizing parameters. Let $v_K$ and $v_L$ be normalized additive valuations of $K$ and $L$, respectively, so that $v_K(K^\times) = v_L(L^\times) = \mathbb{Z}$. As both $A$ and $B$ are local Dedekind rings, we must have

$$\mathfrak{p}B = \mathfrak{P}^e$$

where $e$ is the *ramification index* of the extension. This tells us that

$$(\pi)B = (\Pi^e)$$

and hence that there exists a unit $u$ of $B^\times$ such that $\pi = u\Pi^e$. As units have zero additive valuation, we have $v_L(\pi) = e \cdot v_L(\Pi) = e$ and $v_L(K) = e\mathbb{Z}$. Notice that the unique extension $v$ of $v_k$ of the previous theorem satisfies $v(\Pi) = 1/e$ and thus $v = v_L/e$.
Regarding the ramification index of an extension, we will say that $L/K$ is *unramified* if $e = 1$, and we say that $L/K$ is *totally ramified* if $e = [L : K]$.

The following theorem will also appear in the theory that we will develop:

THEOREM 1.4. *Let $K$ be a field with a non-archimedean, complete valuation. Let $A$ be its valuation ring and $\mathfrak{M} = (\pi)$. Let $S$ be a system of representatives of $A/\mathfrak{M}$. Then, for all $k \in K$ there exist unique $a_i \in S$ such that*

$$k = a_{-n}\pi^{-n} + \cdots + a_0 + a_1\pi + \cdots + a_n\pi^n + \cdots$$

*Proof.* Let

$$s_M = \sum_{i=1}^{M} a_i\pi^i.$$

First, we will show that $\{s_M\}_{M\geq 1}$ is a Cauchy series. Since $K$ is a complete field, the sequence must converge to an element of $K$.
Notice that

$$|s_M - s_N| \leq |\pi|^{M+1}, \text{ if } M < N,$$

showing that the sequence $s_M$ is Cauchy. Let $\alpha \in K$. Write $\alpha = \pi^n\alpha_0$ with $\alpha_0$ a unit in the ring of integers $A$. By definition of $S$, we see that there exists an $a_0 \in S$ such that $\alpha_0 - a_0 \in \mathfrak{M}$. Since now $(\alpha_0 - a_0)/\pi \in A$, we can find $a_1 \in S$ such that $(\alpha_0 - a_0)/\pi - a_1 \in \mathfrak{M}$. This provides the existence of an $a_2 \in S$ such that $(\alpha_0 - a_0 - \pi a_1)/\pi^2 - a_2 \in \mathfrak{M}$, etc. In the limit,

$$\alpha_0 = a_0 + a_1\pi + \cdots, \quad \alpha = \pi^n\alpha_0.$$

Note that

$$\left|\sum a_i\pi^i\right| = |\pi^m|$$

if $a_m$ is the first nonzero component, so $\sum a_i\pi^i = 0$ if and only if $a_i = 0$ for all $i$. This proves uniqueness. □

We finish the chapter with the $p$-adic example:

EXAMPLE 1.5. Consider $\mathcal{K} = \mathbb{Q}_p$ and $|a|_p = p^{-v_p(a)}$ where $v_p(a)$ is the standard $p$-adic valuation, and $\{a \in \mathbb{Q}_p \mid |a|_p \leq 1\} = \mathbb{Z}_p$. In this case, $v_p(\mathbb{Q}_p^\times) = \mathbb{Z} \subset \mathbb{R}$ is a discrete set, and hence the valuation is discrete. As expected, the maximal ideal is principal, with $\mathfrak{M} = p\mathbb{Z}_p = (p)$.

Note that since $v_p(\mathbb{Q}_p) = \mathbb{Z} \subset \mathbb{R}$, a uniformizing parameter will have $v_p(\pi) = 1$ (the valuation is normalized). Since $v_p(p) = 1$, $p$ is a local uniformizing parameter of $\mathbb{Q}_p$ (we already knew that because $\mathfrak{M} = (p)$).

Now fix $n > 0$ and consider the extension $\mathcal{K}_{n+1}/\mathcal{K}$ where $\mathcal{K} = \mathbb{Q}_p$ and $\mathcal{K}_{n+1} = \mathbb{Q}_p(\zeta_n)$ where, as defined in the introduction, $\zeta_n$ is a primitive $p^{n+1}$-th root of unity. Note that $[\mathcal{K}_{n+1} : \mathcal{K}] = (p-1)p^n$. Let us show that $\zeta_n - 1$ is a uniformizing parameter for the field $\mathcal{K}_{n+1} = \mathbb{Q}_p(\zeta_n)$: the irreductible polynomial of $\zeta_n$ is the cyclotomic polynomial

$$x^{p^n(p-1)} + x^{p^n(p-2)} + \cdots + x + 1 = \prod_{\substack{i=0 \\ (i,p)=1}}^{p^{n+1}-1} \left(x - \zeta_n^i\right).$$

The uniqueness of the extension of the valuation gives us that $v_p(1-\zeta_n) = v_p(\sigma(1-\zeta_n))$ where $v_p$ is the extension of the standard $p$-adic valuation to $\mathbb{Q}_p(\zeta_n)$ and $\sigma \in \mathrm{Gal}(\mathcal{K}_{n+1}/\mathcal{K})$ (since $v_p$ and $v_p \circ \sigma$ coincide over $\mathbb{Q}_p$). Thus $v_p(1-\zeta_n) = v_p(1-\zeta_n^i)$, and

$$1 = v_p(p) = p^n(p-1)v_p(1-\zeta_n)$$

so finally

$$v_p(1-\zeta_n) = \frac{1}{p^n(p-1)}$$

and $1 - \zeta_n$ is a uniformizing parameter. This also shows that $e = (p-1)p^n = [\mathcal{K}_{n+1} : \mathcal{K}]$, so $\mathcal{K}_{n+1}/\mathcal{K}$ is totally ramified.

# Chapter 2
# Structure theory

## 1. The Iwasawa algebra

The aim of this chapter is to prove a structure theorem for a certain kind of modules over the algebra

$$\Lambda = \mathbb{Z}_p[[T]] = \left\{ \sum_{i \geq 0} a_i T^i \text{ with } a_i \in \mathbb{Z}_p \right\}$$

which will be called the *Iwasawa algebra* from now on. Note that by Hilbert's basis theorem $\Lambda$ is a Noetherian ring.

We will follow [**18**, §13.2] for the proof of the structure therorem of $\Lambda$-modules that will be presented in this chapter. We will also include some results (such as the $p$-adic Weierstrass preparation theorem) that can be found in [**18**, §7.1] with more generality. An alternative reference is [**14**, §3.1], which presents a more conceptual proof, using more advanced techniques from commutative and homological algebra.

We will start with a key definition:

Definition 2.1 (Distinguished polynomial). *We say that a nonconstant polynomial $P(T) \in \Lambda$ is* distinguished *if*

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

*where $p | a_i$ for $0 \leq i \leq n-1$.*

This concept leads us to a theorem we will widely use:

Theorem 2.2 ($p$-adic Weierstrass preparation theorem). *Let $f(T) \in \Lambda$ be a nonzero power series. Then there exists a unique distinguished polynomial $P(T)$, a unique unit $U(T) \in \Lambda^\times$ an a unique non-negative integer $m$ such that*

$$f(T) = p^m P(T) U(T).$$

Notice that if $f$ is a polynomial then so is $U \in \Lambda^\times$. The following corollary will help in many proofs:

COROLLARY 2.3. *Either $f(T) \in \Lambda$ is the zero power series or it has only finitely many roots.*

*Proof.* Assume that $f(T) \in \Lambda$ is not the zero power series and that has infinitely many roots. The Weierstrass preparation theorem gives a decomposition

$$f(T) = p^m P(T) U(T)$$

where $P$ is a polynomial (and hence it can only have finitely many roots) and $U$ is a unit of the Iwasawa algebra (which can not have roots), reaching a contradiction. □

In order to prove the Weierstrass preparation theorem we have to prove the division lemma, which has interest for itself:

LEMMA 2.4 (Division lemma). *If $f(T), g(T) \in \Lambda$ and $f(T) = a_0 + a_1 T + \cdots$ is such that $p \mid a_i$ for $0 \leq i \leq n-1$ and $a_n \in \mathbb{Z}_p^\times$, then we may uniquely write*

$$g(T) = q(T) f(T) + r(T)$$

*with $r(T) \in \mathbb{Z}_p[T]$ and $\deg r(T) < n$ (with the usual convention that $\deg 0 = -\infty$).*

*Proof.* We will first prove uniqueness, which can be reduced to considering $qf + r = 0$. If both $q, r \neq 0$, we may assume that either $p \nmid r$ or $p \nmid q$. Reduction mod $p$ shows that $p \mid r$, so $p \mid qf$. It can be easily shown that $p \nmid f$, therefore $p \mid q$ which is a contradiction and we must have $q = r = 0$.
Proving existence is a little more difficult. Define $\tau = \tau_n : \Lambda \to \Lambda$ by

$$\tau \left( \sum_{i=0}^{\infty} b_i T^i \right) = \sum_{i=n}^{\infty} b_i T^{i-n}.$$

One may look at $\tau$ as a "shift operator". Clearly $\tau$ is $\mathbb{Z}_p$ linear and satisfies

(1) $\tau(T^n h(T)) = h(T)$ for all $h(T) \in \Lambda$;
(2) $\tau(h(T)) = 0 \iff h(T) \in \mathbb{Z}_p[T]$ with $\deg h \leq n-1$.

We may write

$$f(T) = pP(T) + T^n U(T)$$

where $P(T)$ is a polynomial of degree less than $n$ and $U(T) = a_n + a_{n+1} T + \cdots = \tau(f(T))$. Since $a_n \in \mathbb{Z}_p^\times$, $U(T)$ is a unit of the power series ring. Let

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j p^j \left( \tau \circ \frac{P}{U} \right)^j \circ \tau(g).$$

Notice that possibly all summands contribute, say, to the constant term, but the factor $p^j$ makes the sum of that contributions converge, so $q(T)$ is a well-defined power series in $\Lambda$. Since $qf = pqP + T^n qU$ we have

$$\tau(qf) = p\tau(qP) + \tau(T^n qU) = p\tau(qP) + qU$$

but then

$$p\tau(qP) = p \left( \tau \circ \frac{P}{U} \right) \circ \left( \sum_{j=0}^{\infty} (-1)^j p^j \left( \tau \circ \frac{P}{U} \right)^j \circ \tau(g) \right) = \tau(g) - qU.$$

Therefore $\tau(qf) = \tau(g)$. By the properties of $\tau$ $g = qf + r$, where $\deg r \leq n-1$. This completes the proof of the lemma. □

A particular case of the previous theorem that will be interesting for us is the case where $f$ is a distinguished polynomial, which satisfies automatically the hypothesis. Now we are ready to prove the Weierstrass preparation theorem:

*Proof of the Weierstrass preparation theorem (theorem 2.2).* The factor $p^m$ can be extracted by factoring out the largest possible power of $p$ from the coefficients of $f$.
Now we can assume without losing generality that $f$ has a nonzero coefficient not divisible by $p$. Let $a_n$ be the smallest such coefficient, and let $g(T) = T^n$. The division lemma yields

$$T^n = q(T)f(T) + r(T), \quad \deg r \leq n-1. \tag{2.1}$$

Since

$$q(T)f(T) \equiv q(T)(a_n T^n + \text{ higher terms }) \pmod{p},$$

we must have $r(T) \equiv 0 \pmod{p}$. Therefore $P(T) = T^n - r(T)$ is a distinguished polynomial of degree $n$. Let $q_0$ be the constant term of $q(T)$. Comparing coefficients of $T^n$ in (2.1), we have $1 \equiv q_0 a_n \pmod{p}$. Therefore $q_0 \in \mathbb{Z}_p^\times$, so $q(T)$ is a unit. Let $U(T) = 1/q(T)$. Now $f(T) = P(T)U(T)$, as desired: since any distinguished polynomial of degree $n$ can be written as $P(T) = T^n - r(T)$ we may transform $f(T) = P(T)U(T)$ back to

$$T^n = U(T)^{-1}f(T) + r(T).$$

Regarding uniquness, the uniqueness provided by the division lemma implies uniqueness for $U$ and $P$ here, so we are done. □

All of the above allow us to conclude that $\Lambda$ is a unique factorization domain, whose irreducible elements are $p$ and the irreducible distinguished polynomials. Units are power series with constant term in $\mathbb{Z}_p^\times$. Notice that the division algorithm we presented resembles an Euclidean division and this may induce us to think that $\Lambda$ is in fact an Euclidean space. As we will see, $\Lambda$ is not even a principal ideal domain, so the condition that the divisor $P(T)$ is distinguished is necessary for the division algorithm to work.

We will now introduce some results about the structure of $\Lambda$:

LEMMA 2.5. *Suppose $f, g \in \Lambda$ are relatively prime (in the sense that they have no common factor). Then the ideal $(f, g)$ is of finite index in $\Lambda$.*

*Proof.* Let $h \in (f, g)$ be of minimal degree. Then, because of the Weiestrass preparation theorem, $h = p^s H$ with either $H = 1$ or $H$ distinguished. Suppose $H \neq 1$. Since $f$ and $g$ are relatively prime, we can assume without losing generality that $H$ does not divide $f$. But then, by the division algorithm,

$$f = Hq + r, \quad \deg r < \deg H = \deg h$$

so

$$p^s = hq + p^s r.$$

Since $p^s f, hq \in (f, g)$, we have that $p^s r \in (f, g)$ and $\deg(p^s r) < \deg h$, contradicting the minimality of the degree of $h$.

Therefore $H = 1$ and $h = p^s$. Without losing generality, we may assume that $f$ is not divisible by $p$ and is distinguished. Otherwise we could use $g$ or divide by a unit. Now we have

$$\Lambda \supset (f, g) \supseteq (p^s, f)$$

where inclusions are of finite index. By the division algorithm, any element of $\Lambda$ is congruent mod $f$ to a polynomial of degree less than $\deg f$. Since there are only finitely many such polynomials $\mod p^s$, the ideal $(p^s, f)$ has finite index, so the proof is complete. □

LEMMA 2.6. *Suppose $f, g \in \Lambda$ are relatively prime. Then*

*(1) the natural map*

$$\Lambda/(fg) \longrightarrow \Lambda/(f) \oplus \Lambda/(g)$$

*is an injection with finite cokernel;*

*(2) there is an injection*

$$\Lambda/(f) \oplus \Lambda/(g) \longrightarrow \Lambda/(fg)$$

*with finite cokernel.*

*Proof.* (1) The map is an injection because $\Lambda$ is a unique factorization domain. Now consider $(a \mod f, b \mod g)$. If $a - b \in (f, g)$ then $a - b = fA + gB$ for some $A, B$. Now let

$$c = a - fA = b + gB$$

Then

$$c \equiv a \mod f, \quad c \equiv b \mod g,$$

so $(a, b)$ is in the image. Now recall that for all $(a, b) \in \Lambda/(f) \oplus \Lambda/(g)$ it holds $(a, b) \cong (0, c) \mod (f, g)$ for some $c$. Let $r_1, \ldots, r_n$ be a system of representatives for $\Lambda/(f, g)$. It follows that

$$\{(0 \mod f, r_j \mod g), 1 \leq j \leq n\}$$

is a set of representatives for the cokernel.
(2) From (1),

$$\Lambda/(fg) \cong M \subseteq \Lambda/(f) \oplus \Lambda/(g) = N$$

the inclusion being given by the map $c \mapsto (a, b)$, and $M$ being of finite index in $N$. Let $P$ be any distinguished polynomial in $\Lambda$ relatively prime to $fg$. Then $P$ defines a map $N \to N : (x, y) \mapsto (P(x), P(y))$. If $(x, y) \in N$, then

$$(P^i)(x, y) \equiv (P^j)(x, y) \mod M$$

for some $i < j$. Therefore $1 - P^{j-i} \in \Lambda^\times$ and since $(1 - P^{j-i})P^i(x, y) \equiv (0, 0) \mod M$ then $P^i(x, y) \equiv (0, 0) \mod M$ and we have $P^i(x, y) \in M$.
Since clearly $P(M) \subseteq M$, it follows that $P^k N \subseteq M$ for some $k$. Suppose $P^k(x, y) = 0$ in $N$, so $f \mid P^k x$ and $g \mid P^k y$. Since $P$ and $fg$ are relatively prime, $f \mid x$ and $g \mid y$ which yields $(x, y) = 0$ in $N$. We have proved that the map $P^k : N \to M \cong \Lambda/(fg)$ is injective. The image must contain the ideal $(P^k, fg)$ which is of finite index. This concludes the proof. □

PROPOSITION 2.7. *The prime ideals of $\Lambda$ are*

*(1) the 0 ideal;*

*(2) $(p)$;*

*(3) (P(T)) where $P(T)$ is an irreducible distinguished polynomial;*
*(4) (p, T), which is the unique maximal ideal of $\Lambda$.*

*In particular, $\Lambda$ is a local ring.*

*Proof.* It is obvious that all of the above ideals are prime. It remains to check that all prime ideals have that form. Let $\mathfrak{p} \neq 0$ be a prime ideal, and let $h \in \mathfrak{p}$ be of minimal degree. As we have seen in other occasions, then $h = p^s H$ with either $H =!$ or $H$ distinguished. Since $\mathfrak{p}$ is prime, either $p \in \mathfrak{p}$ or $H \in \mathfrak{p}$. If $H \neq 1$ and $H \in \mathfrak{p}$ then $H$ must be irreducible by minimality of the degree. Therefore we have in both cases $(f) \subseteq \mathfrak{p}$ where $f = p$ or $f$ is irreducible and distinguished. If $(f) = \mathfrak{p}$ then $\mathfrak{p}$ is in the list so we are done. If $(f) \neq \mathfrak{p}$, there exists a $g \in \mathfrak{p}$ with $f \nmid g$. Since $f$ is irreducible, $f$ and $g$ are relatively prime. By a previous lemma, $\mathfrak{p}$ is of finite index in $\Lambda$. Since $\Lambda/\mathfrak{p}$ is a finite $\mathbb{Z}/p\mathbb{Z}$-module, $p^N \in \mathfrak{p}$ for large $N$, so $p \in \mathfrak{p}$ since $\mathfrak{p}$. Also $T^i \equiv T^j \mod \mathfrak{p}$ for some $i < j$, and that means that $1 - T^{j-i} \in \Lambda^\times$, so $T^i \in \mathfrak{p}$ and $T \in \mathfrak{p}$, so $(T, p) \subseteq \mathfrak{p}$. But now $\Lambda/(p, T) = \mathbb{Z}/p\mathbb{Z}$ and therefore $(p, T)$ is maximal and $\mathfrak{p} = (p, T)$. Finally, since all prime ideals are contained in $(p, T)$ it is the only maximal ideal. □

We will equip $\mathbb{Z}_p[[T]]$ with the $(p, T)$-adic topology. Thus $\mathbb{Z}_p[[T]]$ is a topological ring. Let $P_n(T) = (1 + T)^{p^n} - 1$. Then $\{(P_n(T))\}_{n \geq 1}$ is a basis of open neighborhoods of 0.

Lemma 2.8. *We have*

$$\mathbb{Z}_p[[T]] \cong \lim_{\leftarrow} \mathbb{Z}_p[T]/P_n(T).$$

*Thus $\mathbb{Z}_p[[T]]$ is* complete *in the $(p, T)$-adic topology.*

*Proof.* It is clear that $P_n(T)$ is a distinguished polynomial. Further, we claim that $P_n(T) \in (p, T)^{n+1}$. Indeed, $P_0(T) \in (p, T)$ and

$$\frac{P_{n+1}(T)}{P_n(T)} = (1 + T)^{p^n(p-1)} + (1 + T)^{p^n(p-2} + \cdots + 1 \in (p, T),$$

so the claim holds by induction.

By the division lemma (lemma 2.4), there is a natural map from $\mathbb{Z}_p[[T]]$ to $\mathbb{Z}_p[T] \mod P_n(T)$ for each $n$. Namely, $f(T) \mapsto f_n(T)$, where $f(T) = q_n(T)P_n(T) + f_n(T)$ with $\deg f_n < p^n$. If we consider $m \geq n \geq 0$, we have that

$$f_m(T) - f_n(T) - \left(q_n - \frac{P_m}{P_n} q_m\right) P_n = 0.$$

We now claim that $P_m/P_n \in \mathbb{Z}_p[T]$ and therefore that $f_m \equiv f_n \pmod{P_n}$ as polynomials. To prove this claim, we will prove the following more general statement: if $P(T) \in \mathbb{Z}_p[T]$ is a distinguished polynomial, $g(T) \in \mathbb{Z}_p[T]$ is an arbitrary polynomial and $g(T)/P(T) \in \mathbb{Z}_p[[T]]$ then $g(T)/P(T) \in \mathbb{Z}_p[[T]]$. Let $g(T) = f(T)P(T)$ for some $f(T) \in \mathbb{Z}_p[[T]]$, and let $x \in \mathbb{C}_p$ be a zero of $P(T)$. Then

$$0 = P(x) = x^n + ph(x), \ \deg h(T) < n,$$

so $|x| < 1$. Hence $f(x)$ converges, so $g(x) = 0$. We can now divide by $T - x$ and iterate this process, in a larger ring if necessary, to find that $P(T)$ divides $g(T)$ as polynomials. This finishes the proof of the claim.

Now $f_m \equiv f_n \pmod{P_n}$ as polynomials and therefore

$$(f_0, f_1, \ldots) \in \lim_{\leftarrow} \mathbb{Z}_p[T]/(P_n(T)).$$

This gives us the map from the power series ring to the inverse limit. If $f_n = 0$ for all $n$ then $P_n$ divides $f$ for all $n$. Therefore $f \in \cap_{n=0}^{\infty}(p, T)^{n+1} = 0$, so the map is injective.

We want to check that it is surjective. Take $(f_0, f_1, \ldots)$ from the inverse limit. Then, for $m \geq n \geq 0$, we have that $f_m \equiv f_n \pmod{P_n}$ so $f_m \equiv f_n \pmod{(p, T)^{n+1}}$. Therefore, constant terms are congruent $\mod p^{n+1}$, linear terms $\mod p^n$, etc. Therefore the coefficients of the terms form a Cauchy sequence. Let $f(T) = \lim f_n(T) \in \mathbb{Z}_p[[T]]$. We want to show that $f \mapsto (f_0, f_1, \ldots)$. If $m \geq n \geq 0$ then $f_m - f_n = q_{m,n}P_n$ for some $q_{m,n} \in \mathbb{Z}_p[T]$. If we take the limit $m \to \infty$, we have that

$$q_{m,n} = \frac{f_m - f_n}{P_n} \to \frac{f - f_n}{P_n} =: q_{\infty,n}.$$

Since $q_{m,n} \in \mathbb{Z}_p[T]$, the limit must be in $\mathbb{Z}_p[[T]]$, so

$$f = P_n q_{\infty,n} + f_n$$

and $f \mapsto (f_0, f_1, \ldots)$, so we are done. □

We also have the following result, which will be useful in some proofs.

LEMMA 2.9. *Let $f \in \Lambda \setminus \Lambda^{\times}$. Then $\Lambda/(f)$ is infinite.*

*Proof.* Since we may assume $f \neq 0$, then it suffices to consider $f = p$ and $f$ distinguished. If $f = p$, then $\Lambda/(f) \cong \mathbb{Z}/p\mathbb{Z}[[T]]$ which is infinite. For $f$ distinguished, the division algorithm imposes a limit in the degree that the polynomials in the quotient may have, but since the ring of coefficients is $\mathbb{Z}_p$ there are also infinitely many options. □

## 2. Structure of Λ-modules

To state the structure theorem for Λ-modules we need to introduce the concept of pseudoisomorphism:

DEFINITION 2.10 (Pseudoisomorphism). *Two Λ-modules $M$ and $M'$ are said to be* pseudoisomorphic *($M \sim M'$) if there is a homomorphism $M \to M'$ of finite kernel and co-kernel. Equivalently, there exists an exact sequence of Λ-modules*

$$0 \to A \to M \to M' \to B \to 0$$

*with $A$ and $B$ finite Λ-modules.*

There are some relevant comments to be made about the previous definition. First of all, notice that $M \sim M'$ does not imply $M' \sim M$. To see an easy example that proves this fact, consider the ring $\Lambda$ and its maximal ideal $(p, T)$. Then it obviously holds $(p, T) \sim$

$\Lambda$, because $\Lambda/(p,T) \cong \mathbb{Z}/p\mathbb{Z}$ But assume $\Lambda \sim (p,T)$. Let $f(T)$ be the image of 1 by the pseudoisomorphism. The image of $\Lambda$ is $(f) \subseteq (p,T)$, but we have seen that $\Lambda/(f)$ is infinite, thus $(p,T)/(f)$ must be infinite as well. This implies that the cokernel is infinite, contradicting the existence of such a pseudoisomorphism.
However, one can show that for finitely generated $\Lambda$-torsion $\Lambda$-modules $M \sim M'$ holds if, and only if, $M' \sim M$.
The previous results allow us to write

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g), \quad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg).$$

We will devote the rest of this chapter to the proof of the structure theorem of finitely generated $\Lambda$-module, first proved by Iwasawa.

THEOREM 2.11 (Structure of finitely generated $\Lambda$-modules). *Let $M$ be a finitely generated $\Lambda$-module. Then*

$$M \sim \Lambda^r \oplus \left( \bigoplus_{j=1}^{s} \Lambda/(p^{k_j}) \right) \oplus \left( \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}) \right),$$

*where $r, s, t, k_j, m_j \in \mathbb{Z}$ and the $f_j$ are distinguished and irreducible.*

*Proof.* Let us start by noting that this result is the same as the one that can be obtained from modules over principal ideal domains, but here we have only a pseudoisomorphism. This proof will rely on an extension of the techniques that are used to proof the theorem for principal ideal domains.
Since $M$ is finitely generated, take $u_1, \ldots, u_n$ to be its generators. These generators fulfill some relations of the form

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0, \text{ with } \lambda_i \in \Lambda.$$

Let $R$ be the set of relations. Then $R$ is a submodule of $\Lambda^n$ (as each relation is characterized by its $n$ coefficients $\lambda_i$). Since $\Lambda$ is Noetherian, $R$ is finitely generated. Thus we can represent $M$ by a (finite) matrix whose rows are of the form $(\lambda_1, \ldots, \lambda_n)$, where $\lambda_1 u_1 + \cdots \lambda_n u_n = 0$ is a relation. Abusing of the notation, we will use also $R$ to denote that matrix.
Now we will review the basic row and column operators, which correspond to changing the generators of $M$ and $R$.

- OPERATION A. We may permute the rows or permute the columns.
- OPERATION B. We may add a multiple of a row (or column) to another row (column). In particular, this operation allows us to define a "division algorithm": if a row/column is $\lambda' = q\lambda + r$ where $\lambda$ is another row/column, we may replace $\lambda'$ by $r$.
- OPERATION C. We may multiply a row or column by an element of $\Lambda^\times$.

The previous are the classical operations that are used to prove the theorem for modules over principal ideal domains. However, here we are not working in a principal ideal domain, and furthermore we are only looking for a pseudoisomorphism. This allows us to perform three more operations.

- Operation 1. If $R$ contains a row $(\lambda_1, p\lambda_2, \ldots, p\lambda_n)$ with $p \nmid \lambda_1$, then we may change the matrix $R$ to the matrix $R'$ whose first row is $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and the remaining rows are the rows of $R$ with the first elements multiplied by $p$. That is:

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

  As a special case, if $\lambda_2 = \cdots = \lambda_n = 0$ then we may multiply $\alpha_1$, $\beta_1$, ... by an arbitrary power of $p$.
- Operation 2. If all elements in the first column of $R$ are divisible by $p^k$ and there is a row $(p^k\lambda_1, \ldots, p^k\lambda_n)$ with $p \nmid \lambda_1$ then we may change to the matrix $R'$ which is the same as $R$ except that $(p^k\lambda_1, \ldots, p^k\lambda_n)$ is replaced by $(\lambda_1, \ldots, \lambda_n)$. That is:

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

  *Important remark.* Let $R$ be a relations matrix, and let $R'$ be that relation matrix after applying this operation. Let $M_R$ and $M_{R'}$ be the modules represented by the relation submodules $R$ and $R'$, then $M_R \sim M_{R'} \oplus \Lambda/(p^k)$. In the other operations, the module represented by the relation matrix after applying the operation is pseudoisomorphic to the module that one had before applying the operation.
- Operation 3. If $R$ contains a row $(p^k\lambda_1, \ldots, p^k\lambda_n)$, and for some $\Lambda$ with $p \nmid \lambda$ $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ is also a relation (not necessarily explicitly contained in $R$), then we may change $R$ to $R'$, where $R'$ is the same as $R$ but $(p^k\lambda_1, \ldots, p^k\lambda_n)$ is replaced by $(\lambda_1, \ldots, \lambda_n)$.

Hence we have six operations that we will call *admissible*. It is important to notice that all six operations preserve the size of the matrix.
Let $0 \neq f \in \Lambda$. Then, by the Weierstrass preparation theorem,

$$f(T) = p^\mu P(T)U(T),$$

with $P$ distinguished and $U \in \Lambda^\times$. Define the *Weierstrass degree* $\deg_w f$ as follows:

$$\deg_w f = \begin{cases} \infty, & \mu > 0 \\ \deg P(T), & \mu = 0; \end{cases}$$

Now, given a matrix $R$, define

$$\deg^{(k)}(R) = \min_{i,j \geq k} \deg_w(a'_{ij}),$$

where $(a'_{ij})$ ranges over all relation matrices obtained from $R$ via admissible transformations which leave the first $(k-1)$ rows unchanged (notice that we allow opeations that change $a_{ij}$ for all $j$ and $i \geq k$, so we allow also operation which use but do not change the first $(k-1$ rows, such as B).

Assume $R$ has the form

$$\begin{pmatrix} \lambda_{11} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

with $\lambda_{kk}$ distinguished and

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)}(R), \text{ for } 1 \leq k \leq r-1$$

then we asy that $R$ is in $(r-1)$-*normal form.*

After all these definitions, we make the following important claim:

Claim. *If the submatrix $B \neq 0$ then $R$ may be transformed, via admissible transformations, into $R'$ which is in $r$-normal form and has the same first $(r-1)$ diagonal elements.*

*Proof of the claim.* The "special case" of operation 1 allows us to assume, if necessary, that a large power of $p$ divides each $\lambda_{ij}$ with $i \geq r$ and $j \leq r-1$. That is, $p^N | A$, with $N$ large (large enough that $p^N \nmid B$). Using operation 2, we may assume that $p \nmid B$. We may also assume that $B$ contains an entry $\lambda_{ij}$ such that

$$\deg_w(\lambda_{ij}) = \deg^{(r)}(R) < \infty$$

We also may assume that $\lambda_{ij}$ is distinguished, since we know that $\lambda_{ij} = P(T)U(T)$ with $P$ distinguished and $U$ a unit, and we can multiply the $j$-th column bu $U^{-1}$, and since the first $r-1$ rows have zeros in the $j$-th column they do not change. Further, operation $A$ lets us assume that $\lambda_{ij} = \lambda_{rr}$ (again using the existing *zeros*).
By the special case of Operation $B$ (division algorithm) we may assume that $\lambda_{rj}$ is a polynomial with

$$\deg \lambda_{rj} < \lambda_{rr} \text{ for } j \neq r, \text{ and } \deg \lambda_{rj} < \lambda_{jj} \text{ for } j < r.$$

Since $\lambda_{rr}$ has minimal Weierstrass degree in $B$, we must have $p \mid \lambda_{rj}$ for $j > r$. By 1, we may assume $p^N \mid \lambda_{rj}$, $j < r$, for some large $N$. Suppose $\lambda_{rj} \neq 0$ for some $j > r$. Operation 1 allows us to remove the power of $p$ from some nonzero $\lambda_{rj}$ with $j > r$ with the zeros above being left unchanged. Then

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg_w \lambda rr$$

contradicting the minimality of the Weierstrass degree of $\lambda_{rr}$. Thus $\lambda_{rj} = 0$ for $j > r$.
Finally, if some $\lambda_{rj} \neq 0$ for $j < r$, use Operation 1 to obtain $p \nmid \lambda_{rj}$ for some j and notice that

$$\deg_w \lambda_{rj} \leq \deg \lambda_{rj} < \deg \lambda_{jj} = \deg_w \lambda_{jj} = \deg^{(j)}(R),$$

which contradicts the definition of $\deg^{(j)}(R)$. Therefore $\lambda_{rj} = 0$ for $j \neq r$, so the claim is proved. □

If we start with a matrix $R$ and $r = 1$, we may use the claim to successively change $R$ until we obtain a matrix

$$\begin{pmatrix} \lambda_{11} & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \lambda_{rr} & 0 \\ \mathbf{A} & & & \mathbf{0} \end{pmatrix}$$

with each $\lambda_{jj}$ distinguished and $\deg \lambda_{jj} = \deg^{(j)}(R)$ for $j \leq r$. By the division algorithm we may assume that $\lambda_{jj}$ is a polynomial and

$$\deg \lambda_{ij} < \deg \lambda_{jj}, \text{ for } i \neq j.$$

Now suppose $\lambda_{ij} \neq 0$ for some $i \neq j$. Since $\deg_w \lambda_{jj}$ is minimal, then we must have $p \mid \lambda_{ij}$, so we have a nonzero relation $(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$ divisible by $p$. Let $\lambda = \lambda_{11} \cdots \lambda_{rr}$ and notice that $p \nmid \lambda$, since the $\lambda_{jj}$'s are distinguished. Then

$$\left( \lambda \frac{1}{p} \lambda_{i1}, \ldots, \lambda \frac{1}{p} \lambda_{ir}, 0, \ldots, 0 \right)$$

is also a relation since $\lambda_{jj} u_j = 0$. By operation 3 we may assume that $p \nmid \lambda_{ij}$ for some $j$, so

$$\deg_w \lambda_{ij} \leq \deg \lambda_{ij} < \lambda_{jj} = \deg^{(j)}(R),$$

which is impossible. Therefore $\lambda_{ij} = 0$ for all $i, j$ with $i \neq j$, so $\mathbf{A} = \mathbf{0}$. In terms of $\Lambda$-modules, this means

$$\Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}.$$

The desired result follows from adding the factors $\Lambda/(p^k)$ that were discarded in Operation 2. Nonetheless, it is important to notice that $\lambda_{jj}$ may not be irreducible, but that is not a problem since we proved $\Lambda/(fg) \sim \Lambda(f) \oplus \Lambda(g)$. □

If $s, t, m_j, r, f_j$ are as in theorem 2.11, we define

$$\mu(M) = \sum_{i=1}^{s} k_j, \ \lambda(M) = \sum_{j=1}^{t} m_j \deg f_j$$

where $M$ is a finitely generated $\Lambda$-module. Note that $M$ is a $\Lambda$-torsion module if, and only if, $r = 0$. We now introduce a concept that will be of crucial importance in the last chapters of this thesis:

Definition 2.12 (Characteristic ideal). *Let $M$ be a finitely generated torsion $\Lambda$-module. We define the* characteristic ideal *of $M$ as the ideal of $\Lambda$*

$$\mathrm{ch}(M) = \left( p^{\mu} \prod_{j=1}^{t} f_j^{m_j} \right).$$

As proven in [**1**, §7], the characteristic ideal $\mathrm{ch}(M)$ only depends on $M$, and not on the choice of pseudoisomorphism of theorem 2.11. In that same reference one can also find the proof of the following important property of the characteristic ideal:

PROPOSITION 2.13. *Let $M_1, M_2, M_3$ be finitely generated torsion $\Lambda$-modules such that the sequence*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

*is exact. Then*

$$\mathrm{ch}(M_2) = \mathrm{ch}(M_1) \cdot \mathrm{ch}(M_3).$$

## 3. Strucutre of $\Lambda[\Delta]$-modules

In this section $M$ will denote a $\Lambda$-module equipped with an action of a quotient $\Delta$ of $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$. Thus $M$ is a $\Lambda[\Delta]$-module. Let

$$\omega : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times$$

denote a *Teichmuller character*, i.e. the character such that $\omega(a) \equiv a \pmod p$, and let $k$ denote the order of $\Delta$. Write

$$\theta = \omega^{\frac{p-1}{k}} : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times.$$

Note that all homomorphisms $\Delta \to \mathbb{Z}_p^\times$ are given by $\{\theta^i\}_{i=0,1,\dots,k-1}$ and that

$$M = \bigoplus_{i=0}^{k-1} M^{(i)},$$

where

$$M^{(i)} := \left\{ m \in M \,|\, \sigma(m) = \theta^i(\sigma) \cdot m,\ \forall \sigma \in \Delta \right\}.$$

REMARK 2.14. Note that $\Lambda[\Delta]$ is a $\Lambda[\Delta]$-module and therefore

$$\Lambda[\Delta] \cong \bigoplus_{i=0}^{k-1} \Lambda[\Delta]^{(i)} \cong \bigoplus_{i=0}^{k-1} \Lambda.$$

In this more general context we can also introduce the notion of pseudoisomporhism:

DEFINITION 2.15 (Pseudoisomorphism). *We say that two torsion finitely generated $\Lambda[\Delta]$-modules $M$ and $M'$ are* pseudoisomorphic *(and we write $M \sim M'$) if and only if there is $\Lambda[\Delta]$-homomorphism between them with finite kernel and cokernel.*

The structure theorem reads:

THEOREM 2.16. *Let $M$ be a finitely generately torsion $\Lambda[\Delta]$-module. Then*

$$M \sim \bigoplus_{j=1}^{r} \Lambda[\Delta] \Big/ g_j \, \Lambda[\Delta]$$

*where $g_j$ are non-zero divisors in $\Lambda[\Delta]$.*

Notice that this theorem is a generalization of the structure theorem of the previous section (theorem 2.11) and can proven applying theorem 2.11 to the parts of the decomposition of $M$. We can use theorem 2.16 to define the characteristic ideal in this setting:

Definition 2.17 (Characteristic ideal). *Let $M$ be a finitely generated torsion $\Lambda[\Delta]$-module. We define the* characteristic ideal *of $M$ as the ideal of $\Lambda[\Delta]$*

$$\mathrm{ch}_\Delta(M) = (g_1 \cdots g_r).$$

We can also state a version of proposition 2.13 for these characteristic ideals:

Proposition 2.18. *Let $M_1, M_2, M_3$ be finitely generated torsion $\Lambda[\Delta]$-modules such that the sequence*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

*is exact. Then*

$$\mathrm{ch}_\Delta(M_2) = \mathrm{ch}_\Delta(M_1) \cdot \mathrm{ch}_\Delta(M_3).$$

In chapters 4 and 5 we will need to work with this generality.

# Chapter 3
# Iwasawa's control theorem on $\mathbb{Z}_p$-extensions

The aim of this chapter will be to prove an important result due to Iwasawa on the growth of the $p$-part of the class number in field extensions using the structure theorem that we proved in the previous chapter. We will follow the approach of [**18**, §13.3].

## 1. $\mathbb{Z}_p$-extensions

We will start by introducing some concepts and notation that we will use for the rest of the chapter. Fix a number field $F$. A $\mathbb{Z}_p$-*extension* is an extension $F_\infty/F$ with $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, the additive group of $p$-adic integers. We have the following result:

PROPOSITION 3.1. *Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension. Then, for each $n \geq 0$, there is a unique field $F_n$ of degree $p^n$ over $F$, and these $F_n$, plus $F_\infty$, are the fields between $F$ and $F_\infty$.*

*Proof.* The intermediate fields of the extension $F_\infty/F$ correspond to the closed subgroups of $\mathbb{Z}_p$. Let $S \neq 0$ be a closed subgroup and let $x \in S$ be such that $v_p(x)$ is minimal. Then $x\mathbb{Z}$, hence $x\mathbb{Z}_p$, is in $S$. By the choice of $x$, we must have that $S = x\mathbb{Z}_p = p^n\mathbb{Z}_p$ for some $n$. The result follows easily. □

This proposition allows us to regard a $\mathbb{Z}_p$-extension $F_\infty/F$ as a sequence of fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_\infty = \bigcup_{n \geq 0} F_n$$

with

$$\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

The following example shows that each number field has at least a $\mathbb{Z}_p$-extension:.

EXAMPLE 3.2. Denote by $B_n$ the subfield of $\mathbb{Q}(\zeta_n)$ which is cyclic of degree $p^n$ over $\mathbb{Q}$, which is unique (consider the isomorphism $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times C_{p^n}$, where $C_{p^n}$ is a cyclic group of order $p^n$, and let $B_n$ be the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$). Then we have that $B_0 = \mathbb{Q}$ and that $B_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$-extension.
Now let $F$ be any number field and let $F_\infty = FB_\infty$. We claim that $F_\infty/F$ is a $\mathbb{Z}_p$-extension. Let $B_e = F \cap B_\infty$. Then $\mathrm{Gal}(F_\infty/F) \cong \mathrm{Gal}(B_\infty/B_\infty \cap F) \cong p^e\mathbb{Z}_p \cong \mathbb{Z}_p$, as desired. The extension $F_\infty/F$ is called the *cyclotomic* $\mathbb{Z}_p$-*extension* of $F$.

REMARK 3.3. It is a consequence of Class Field Theory (see [**18**, Thm. 13.4]) that the number of independent $\mathbb{Z}_p$-extensions of a number field $F$ is $r_2 + 1 + \delta$, where $r_2$ is the number of pairs of complex conjugate embeddings of $F$ (therefore if $r_1$ denotes the number of real embeddings of $F$, then $[F : \mathbb{Q}] = r_1 + 2r_2$) and $\delta \geq 0$ is called the *Leopoldt's defect*. *Leopoldt's conjecture* states that $\delta = 0$. Leopoldt's conjecture is true for $F/\mathbb{Q}$ abelian (see [**18**, Cor. 5.3]). Therefore, if $F$ is totally real and abelian over $\mathbb{Q}$, it only has the cyclotomic $\mathbb{Z}_p$-extension.

We will denote by $\mathrm{Cl}(F_n)$ the class group of $F_n$ and by $A_n$ the $p$-Sylow of $\mathrm{Cl}(F_n)$. Let $H_n$ be the *Hilbert class field* of $F_n$, so that $\mathrm{Gal}(H_n/F_n) \cong \mathrm{Cl}(F_n)$, and let $L_n$ be the $p$-Hilbert class field of $F_n$, that is, the maximal unramified $p$-extension of $F_n$, so that $\mathrm{Gal}(L_n/F_n) \cong A_n$. Each $L_n$ is Galois over $F$, because $F_n$ is Galois over $F$ and the composition of unramified $p$-extensions is again an unramified $p$-extension. $L_\infty = \bigcup_{n\geq 0} L_n$. Notice that $L_\infty$ is the maximal unramified $p$-extension of $F_\infty$. Now consider the Galois group

$$\mathfrak{G} = \mathrm{Gal}(L_\infty/F) = \varprojlim \mathrm{Gal}(L_n/F).$$

We still need some more notation: let $\Gamma = \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ and let $\gamma_0$ be a topological generator of $\Gamma$, i.e, $\gamma_0$ is such that the cyclic group it generates is dense in $\Gamma$. Notice that the ideal generated by $\gamma_0$ is $\mathbb{Z}$ which is dense in $\mathbb{Z}_p \cong \Gamma$. Define also $Y_n = \mathrm{Gal}(L_n/F_n) \cong A_n = p - \text{Sylow of the ideal class group of } F_n$, and let $Y_\infty = \mathrm{Gal}(L_\infty/F_\infty)$. We have the diagram of figure 3.1.

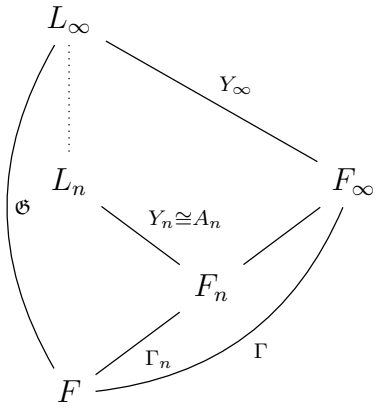


FIG. 3.1. Field extensions defined in chapter 3 and their Galois groups.

We will now introduce a couple of result regarding the ramification of primes in $\mathbb{Z}_p$-extensions:

PROPOSITION 3.4. *Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension and let $\ell$ be a prime (possibly archimedean) of $F$ which does not lie above $p$. Then $F_\infty/F$ is unramified at $\ell$ (in other words, $\mathbb{Z}_p$-extensions are "unramified outside $p$".*

*Proof.* Let $I \subseteq \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$ be the inertia group for $\ell$. Since $I$ is closed, $I = 0$ or $I = p^n\mathbb{Z}_p$ for some $n$. If $I = 0$ we are done, so assume that $I = p^n\mathbb{Z}_p$. In particular, $I$ is

infinite. Since $I$ must have order 1 or 2 for infinite primes, we may assume that $\ell$ is non-archimedean. For each $n$, choose inductively a place $\ell_n$ of $F_n$ lying above $\ell_{n-1}$, with $\ell_0 = \ell$. Let $\overline{F}_n$ be the completion, and let $\overline{F}_\infty = \cup \overline{F}_n$. Then

$$I \subseteq \mathrm{Gal}(\overline{F}_\infty/\overline{F}).$$

Let $U$ be the group of units of $\overline{F}$. Local class field theory says that there is a continuous surjective homomorphism

$$U \to I \cong p^n\mathbb{Z}_p,$$

but

$$U \cong G \times \mathbb{Z}_l^a,\ a \in \mathbb{Z}$$

where $G$ is a finite group and $l$ is the rational prime divisible by $\ell$. This can be proved by considering the map $\log_l : U \to l^{-N}\mathcal{O}$ where $\mathcal{O}$ are the local integers for some $N$. The kernel of this map is finite and $\mathcal{O}$ is a finitely generated free $\mathbb{Z}_l$-module). Since $p^n\mathbb{Z}_p$ has no torsion, we must have a surjective and continuous map

$$\mathbb{Z}_l^a \to p^n\mathbb{Z}_p \to p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

However, $\mathbb{Z}_l^a$ has no closed subgroups of index $p$, so we have a contradiction and we are done. □

PROPOSITION 3.5. *Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension. At least one prime ramifies in this extension, and there exists $n \geq 0$ such that every prime which ramifies in $F_\infty/F_n$ is totally ramified.*

*Proof.* Since the class number of $F$ is finite, the maximal abelian unramified extension of $F$ is finite, so some prime must ramify in $F_\infty/F$. We know that only finitely many primes of $F$ ramify in $F_\infty/F$ by proposition 3.4. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be those primes, and let $I_1, \ldots, I_s$ be the corresponding inertia groups. Then

$$\bigcap I_j = p^n\mathbb{Z}_p$$

for some $n$. The fixed field of $p^n\mathbb{Z}_p$ is $K_n$ and $\mathrm{Gal}(F_\infty/F_n)$ is contained in each $I_j$. Therefore all primes above $\mathfrak{p}_j$ are totally ramified in $F_\infty/F_n$, and we are done. □

Define

$$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(F_n/F)].$$

From now on we endow the Iwasawa algebra $\Lambda$ with the topology defined by the powers of the maximal ideal $(p, T)$. We have the following lemmas:

LEMMA 3.6. *There is an isomorphism $\Lambda(\Gamma) \cong \Lambda$ of topological $\mathbb{Z}_p$-algebras.*

*Proof.* We will construct the isomorphism at finite level an then pass to the limit. Let $\gamma_0^{(n)}$ be the projection of the topological generator $\gamma_0$ to $\mathrm{Gal}(F_n/F)$. We have isomorphisms of $\mathbb{Z}_p$-algebras

$$\begin{array}{rcl} \mathbb{Z}_p[\mathrm{Gal}(F_n/F)] & \cong & \mathbb{Z}_p[T]/P_n(T) \\ \gamma_0^{(n)} & \mapsto & 1+T, \end{array}$$

where as in lemma 2.8 we define $P_n(T) = (1+T)^{p^n} - 1$.

Passing to the limit, this gives

$$\Lambda(\Gamma) = \lim_{\leftarrow} \mathbb{Z}_p[\mathrm{Gal}(F_n/F)] \cong \lim_{\leftarrow} \mathbb{Z}_p[T]/P_n(T).$$

The proof concludes by noting that in lemma 2.8 we showed

$$\mathbb{Z}_p[T]/P_n(T) \cong \Lambda.$$

□

LEMMA 3.7. *$Y_\infty$ is a $\Lambda$-module.*

*Proof.* By the previous lemma, it suffices to see that $Y_\infty$ is a $\Gamma$-module. To do this, let $\gamma \in \Gamma$, and let $\tilde{\gamma} \in \mathfrak{G} = \mathrm{Gal}(L_\infty/F)$ be a lift of $\gamma$. Then define

$$\gamma \cdot y = \tilde{\gamma} y \tilde{\gamma}^{-1}$$

for $y \in Y_\infty$. Since $Y_\infty$ is abelian, it is easy to see that this is a well-defined action. □

## 2. Iwasawa's control theorem

We will use the same notation as in the previous section. Let us denote by $e_n$ the number such that $p^{e_n}$ is the exact power of $p$ dividing the class number of $F_n$, i.e., $e_n = v_p(\#A_n)$. Using this notation, the Iwasawa control theorem is stated as follows:

THEOREM 3.8 (Iwasawa control theorem). *There exist integers $\lambda \geq 0$, $\mu \geq 0$, and $\nu$, all independent of $n$, and an integer $n_0$ such that*

$$e_n = \lambda n + \mu p^n + \nu \text{ for all } n \geq n_0$$

We already know (lemma 3.7) that $Y_\infty$ is a $\Gamma$-module and hence a $\Lambda$-module. We will show that this $\Lambda$-module is finitely generated and $\Lambda$-torsion, and thus pseudoisomorphic (by the previous chapter) to a direct sum of modules of the form $\Lambda/(p^k)$ and $\Lambda/(P(T)^k)$. Once we have proved that, it will be easy to see what happens at the $n$-th level for these modules. By proposition 3.4, only primes above $p$ can ramify, and by proposition 3.5, there are only finitely many ramified primes in $F_\infty/F$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes that ramify in $F_\infty/F$.

We will now work under an assumption and work the proof of lemma 3.7 under that assumption. It will give us more information about the behaviour at finite levels:
ASSUMPTION: *All primes which are ramified in $F_\infty/F$ are totally ramified.*
Assuming this is to assume that $n = 0$ with $F_0 = F$ in proposition 3.5. In general, by that same lemma, such a setting can be accomplished by replacing $F$ by $F_m$ for some $m$. By the assumption, $F_{n+1} \cap L_n$ is a simultaneously unramified and totally ramified extension of $F_n$, so $1 = [F_{n+1} \cap L_n : F_n]$, thus $F_{n+1} \cap L_n = F_n$ and $\mathrm{Gal}(L_n/F_n) \cong \mathrm{Gal}(L_n F_{n+1}/F_{n+1})$ which is a quotient of $Y_{n+1}$. Hence, we have a map

$$Y_{n+1} \longrightarrow Y_n$$

which corresponds to the norm map $A_{n+1} \longrightarrow A_n$ on ideal class groups. Observe that

$$Y_n \cong \mathrm{Gal}(L_n F_\infty/F_\infty),$$

so

$$\varprojlim Y_n \cong \varprojlim \mathrm{Gal}\left(\left(\bigcup L_n F_\infty\right)/F_\infty\right) = \mathrm{Gal}(L/F_\infty) = Y_\infty.$$

Let $\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n}$. Extend $\gamma$ to $\tilde{\gamma} \in \mathrm{Gal}(L_n/F)$. Let $y \in Y_n$. Then $\gamma$ acts on $y$ by $y^\gamma = \tilde{\gamma} y (\tilde{\gamma})^{-1}$ (throughout this proof we will use this notation for group actions, as it makes expressions more compact). Since $\mathrm{Gal}(L_n/F_n)$ is abelian, $y^\gamma$ is well-defined. Therefore $Y_n$ becomes a $\mathbb{Z}_p[\Gamma_n]$-module. Representing an element of $Y_\infty \cong \varprojlim Y_n$ as a vector $(y_0, y_1, \ldots)$, and letting $\mathbb{Z}_p[\Gamma_n]$ act on the $n$-th component, we can easily find that $Y_\infty$ becomes a modules over $\Lambda \cong \varprojlim \mathbb{Z}_p[\Gamma_n]$, since the only thing to be checked is that $y^\gamma \in Y$, which is clear.

Recall that we denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ the primes which ramify in $F_\infty/F$, and fix a prime $\tilde{\mathfrak{p}}_i$ of $L$ lying above $\mathfrak{p}_i$. Let $I_i \subseteq G$ be the inertia group. Since $L_\infty/F_\infty$ is unramified, $I_i \cap Y_\infty = 1$, and since $F_\infty/F$ is totally ramified at $\mathfrak{p}_i$, $I_i \hookrightarrow \mathfrak{G}/Y_\infty = \Gamma$ is surjective, hence bijective. So $G = I_i Y_\infty = Y_\infty I_i$ for $i = 1, \ldots, s$. Let $\sigma_i \in I_i$, map to $\gamma_0$. Then $\sigma_i$ must be a topological generator $I_i$, and since $I_i \subseteq Y_\infty I_1$ we have $\sigma_i = a_i \sigma_1$ for some $a_i \in Y_\infty$. Note that $a_1 = 1$.

Now we will state some useful technical lemmas, *which are true under the conditions of the assumption above.*

LEMMA 3.9. *Let $G'$ be be the closure of the commutator subgroup of $\mathfrak{G}$. Then*

$$G' = Y_\infty^{\gamma_0 - 1} = T Y_\infty.$$

*Proof.* Since $\Gamma \cong I_1 \subseteq \mathfrak{G}$ maps onto $\Gamma = \mathfrak{G}/Y_\infty$, we can lift $\gamma \in \Gamma$ to the corresponding element in $I_1$ in order to define the action of $\Gamma$ on $Y_\infty$. For simplicity, we may identify $\Gamma$ and $I_1$, so $y^\gamma = \gamma y \gamma^{-1}$. Now let

$$a = \alpha x, b = \beta y, \text{ with } \alpha, \beta \in \Gamma,\ x, y \in Y_\infty,$$

be arbitrary elements of $\mathfrak{G} = \Gamma Y_\infty$. Then

$$aba^{-1}b^{-1} = \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^\alpha \alpha\beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} =$$
$$x^\alpha (y x^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1}\ \beta^{-1} = x^\alpha (y x^{-1})^{\alpha\beta} (y^{-1})^\beta = (x^\alpha)^{1-\beta} (y^\beta)^{\alpha - 1}.$$

Now let $\beta = 1$ and $\alpha = \gamma_0$. This results in $y^{\gamma_0 - 1} \in G'$, so $Y_\infty^{\gamma_0 - 1} \subseteq G'$. Now for arbitrary $\beta$, there exists $c \in \mathbb{Z}_p$ with $\beta = \gamma_0^c$, so

$$1 - \beta = 1 - \gamma_0^c = 1 - (1+T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Gamma,$$

since we know that $\gamma_0 - 1 = T$ then $(x^\alpha)^{1-\beta} \in Y_\infty^{\gamma_0 - 1}$. One can show in a similar manner that $(y^\beta)^{1-\alpha} \in Y_\infty^{\gamma_0 - 1}$. But $Y_\infty^{\gamma_0 - 1} = T Y_\infty$ is closed (as it is the image of the compact set $Y_\infty$), and thus $G' \subseteq Y_\infty^{\gamma_0 - 1}$. □

LEMMA 3.10. *Let $Z_0$ be the $\mathbb{Z}_p$-submodule of $Y_\infty$ generated by $\{a_i | 2 \le i \le s\}$ and by $Y_\infty^{\gamma_0 - 1} = T Y_\infty$. Let $Z_n = \nu_n Z_0$, where*

$$\nu_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}.$$

*Then $Y_n \cong Y_\infty / Z_n$ for $n \ge 0$.*

*Proof.* Consider the case $n = 0$. We have $F \subseteq L_0 \subseteq L_\infty$. Since $L_0$ is the maximal unramified $p$-extension of $F$ and $L_\infty/F$ is a $p$-extension, $L_0/F$ is the maximal unramified abelian subextension of $L_\infty/F$. Therefore $\mathrm{Gal}(L_\infty/L_0)$ must be the closed subgroup of $\mathfrak{G}$ generated by $G'$ and all the inertia groups $I_i$ for $1 \leq i \leq s$. Thus $\mathrm{Gal}(L_\infty/L_0)$ is the closure of the group generated by $Y_\infty^{\gamma_0 - 1}$, $I_1$ and $a_2, \ldots, a_s$, so

$$Y_0 = \mathrm{Gal(L_0/F)} = \mathfrak{G}/\mathrm{Gal}(L_\infty/L_0) = Y_\infty I_1/\mathrm{Gal}(L_\infty/L_0) \cong$$

$$\cong Y_\infty/\overline{\langle Y_\infty^{\gamma_0 - 1}, a_2, \ldots, a_s\rangle} = Y_\infty/Z_0.$$

Now suppose $n \geq 1$. Replace $F$ by $F_n$ and $\gamma_0$ by $\gamma_0^{p^n}$. Then $\sigma_i$ becomes $\sigma_i^{p^n}$. Notice that

$$\sigma_i^{k+1} = (a_i\sigma_1)^{k+1} = a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^k a_i \sigma_1^{-k}\sigma_1^{k+1} = a_i^{1+\sigma_1+\cdots+\sigma_1^k}\sigma_1^{k+1}.$$

Therefore

$$\sigma_i^{p^n} = (\nu_n a_i)\sigma_1^{p^n},$$

so $a_i$ is replaced by $\nu_n a_i$. Finally, $Y_\infty^{\gamma_0 - 1}$ is replaced by $(\gamma_0^{p^n} - 1)X = \nu_n Y_\infty^{\gamma_0 - 1}$. Therefore $Z_0$ becomes $\nu_n Z_0$ which yields the desired result. □

Now we recall the famous Nakayama's lemma, which will be also useful for our proof:

Lemma 3.11 (Nakayama's lemma). *Let $X$ be a compact $\Lambda$-module. Then $X$ is finitely generated over $\Lambda$ if, and only if, $X/(p,T)X$ is finite. If $x_1, \ldots, x_n$ generate $X/(p,T)X$ over $\mathbb{Z}$, then they also generate $X$ as a $\Lambda$-module. As a special case, $X/(p,T)X = 0 \iff X = 0$.*

Lemma 3.12. *$Y_\infty = \mathrm{Gal}(L_\infty/F_\infty)$ is a finitely generated $\Lambda$-module.*

*Proof.* Clearly $\nu_1 \in (p,T)$ , so $Z_0/(p,T)Z_0$ is a quotient of $Z_0/\nu_1 Z_0 = Z_0/Z_1 \subseteq Y_\infty/Z_1 = Y_1$, which is finite, so by Nakayama's lemma $Y_0$ is finitely generated. Since $Y_\infty/Z_0 = Y_0$ is finite, and since $\Lambda$ is a Noetherian ring this means that $Y_\infty$ is finitely generated. □

Arbitrary $F$. Now consider the general setting. Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension and let $e \geq 0$ be such that all ramified primes in $F_\infty/F_e$ are totally ramified. Then the lemmas that we proved under the assumption apply to $F_\infty/F_e$. In particular, $Y_\infty$, which is the same for $F_e$ and $F$, is a finitely generated $\Lambda$-module, and for $n \geq e$ we have

$$1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e} = \frac{\nu_n}{\nu_e} = \nu_{n,e}$$

since now $\gamma_o^{p^e}$ is a topological generator for $\mathrm{Gal}(F_\infty/F_e)$. Now let $Z_e$ play for $F_e$ the same role that $Z_0$ played for $F$. Then

$$Z_n = \nu_{n,e} Z_e, \text{ and } Y_n \cong Y_\infty/Z_n \text{ for } n \geq e.$$

Hence we proved the following lemma:

Lemma 3.13. *Let $F_\infty/F$ be a $\mathbb{Z}_p$-extension. Then $Y_\infty$ is a finitely generated $\Lambda$-module, and there exists $e \geq 0$ such that*

$$Y_n \cong Y_\infty/\nu_{n,e} Z_e \text{ for all } n \geq e.$$

We can now apply the structure theorem for $\Lambda$-modules to $Y_\infty$. We can also apply it to $Z_e$ with the same answer since $Y_\infty/Z_e$ is finite. This yields

$$Z_e \sim Y_\infty \sim \Lambda^r \oplus \left(\bigoplus_j \Lambda/(p^{k_j})\right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j})\right).$$

We will now look at the growth of the $p$-part of the class number for modules of this kind:

PROPOSITION 3.14. *Let $E$ be a finitely generated $\Lambda$-module such that*

$$E = \Lambda^r \oplus \left(\bigoplus_j \Lambda/(p^{k_j})\right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j})\right)$$

*where each $f_j(T)$ is distinguished. Let $\mu = \sum_j k_j$ and $\lambda = \sum_j m_j \deg f_j$. If $E/\nu_{n,e}E$ is finite for all $n$, then $r = 0$ and there exist $n_0$ and $\nu$ such that*

$$|E/\nu_{n,e}E| = p^{\mu p^n + \lambda n + \nu}, \text{ for all } n > n_0.$$

*Proof.* Let us take a look at all the possible summands:

(1) $V = \Lambda$. By lemma 2.9, since $\nu_{n,e} \notin \Lambda^\times$ by definition then $\Lambda/\nu_{n,e}$ is infinite. But $E/\nu_{n,e}E$ is finite, so $\Lambda$ cannot occur as a summand.

(2) $V = \Lambda/(p^k)$. In this case

$$V/\nu_{n,e} \cong \Lambda/(\nu_{n,e}, p^k).$$

It is easy to see (by the Weierstrass Preparation Theorem) that if the quotient of two distinguished polynomials is a polynomial, then it is distinguished or constant. Thus

$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = \frac{((1+T)^{p^n} - 1)/T}{((1+T)^{p^e} - 1)/T}$$

is a distinguished polynomial. Therefore, by the division algorithm, every element of $\Lambda/(p^k, \nu_{n,e})$ is represented uniquely by a polynomial mod $p^k$ of degree less than $\deg \nu_{n,e} = p^n - p^e$. Hence

$$|V/\nu_{n,e}V| = p^{k(p^n - p^e)} = p^{kp^n + c},$$

where $c$ is a constant.

(3) $V = \Lambda/(f(T)^m)$ with $f$ distinguished. Let $g(T) = f(T)^m$. Now $g$ is also distinguished, say of degree $d$. Now $T^d \equiv pQ(T) \pmod g$ for some polynomial $Q(T)$, and $T^k \equiv p(\text{polynomial}) \pmod g$ for $k \geq d$. Therefore if $p^n \geq d$ then

$$(1+T)^{p^n} = 1 + p(\text{polynomial}) + T^{p^n} \equiv 1 + p(\text{polynomial}) \pmod g.$$

Now, expanding the binomial

$$(1+T)^{p^{n+1}} \equiv 1 + p^2(\text{polynomial}) \pmod g.$$

Now we can write

$$P_{n+2}(T) := (1+T)^{p^{n+2}} - 1 = ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1)((1+T)^{p^{n+1}} - 1) \equiv$$
$$\equiv (p + p^2(\text{polynomial}))P_{n+1}(T) \equiv p(1 + p(\text{polynomial}))P_{n+1}(T) \pmod g.$$

But $1 + p(\text{polynomial}) \in \Lambda^\times$, so $P_{n+2}/P_{n+1}$ acts as $p(\text{unit})$ on $V = \Lambda/(g)$ for $p^n \geq d$. Now assume $n_0 > e$, $p^{n_0} \geq d$ and $n \geq n_0$. Then

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}}$$

and

$$\nu_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1,e}V) = p\nu_{n+1,e}V.$$

Thus $|V/\nu_{n+2}V| = |V/pV||pV/p\nu_{n+1,e}V|$ for $n \neq n_0$. Notice that $(g,p) = 1$ and therefore the multiplication by $p$ is injective, so $|pV/p\nu_{n+1,e}V| = |V/\nu_{n+1,e}V|$. But we had $V/pV \cong V/(p,g) \cong \Lambda/(p,T^d)$, which yields $|V/pV| = p^d$. By induction

$$|V/\nu_{n,e}V| = p^{d(n-n_0-1)}|V/\nu_{n_0+1,e}V|$$

for $n \geq n_0 + 1$. Now if $V/\nu_{n,e}V$ is finite then

$$|V/\nu_{n,e}V| = p^{dn+c} \text{ for } n \geq n_0 + 1$$

for some constant $c$. If $V/\nu_{n,e}V$ is infinite then $V$ cannot occur. This happens when $f$ and $\nu_{n,e}$ are not coprime, by the previous chapter.

□

We now have an exact sequence

$$0 \to A \to Z_e \to E \to B \to 0$$

where $A$ and $B$ are finite and $E$ is as in the previous proposition. Hence we know the order of $E/\nu_{n,e}E$ for all $n > n_0$. We want to obtain a similar result for $Z_e$. All we can conclude at the moment is that $e_n = \mu p^n + \lambda n + c_n$ where $c_n$ is bounded. To establish the final result we will use the following lemma:

LEMMA 3.15. *Suppose $Z$ and $E$ are $\Lambda$-modules with $Z \sim E$ such that $Z/\nu_{n,e}Z$ is finite for all $n \geq e$. Then, for some constant $c$ and some $n_0$,*

$$|Z/\nu_{n,e}Z| = p^c|E/\nu_{n,e}E| \text{ for all } n \geq n_0.$$

*Proof.* We have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Z & \longrightarrow & Z & \longrightarrow & Z/\nu_{n,e}Z & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}E & \longrightarrow & E & \longrightarrow & E/\nu_{n,e}E & \longrightarrow & 0 \end{array}$$

With the following inequalities:

(1) $|\ker(\phi'_n)| \leq |\ker(\phi)|$
(2) $|\text{coker}(\phi'_n)| \leq |\text{coker}(\phi)|$
(3) $|\text{coker}(\phi''_n)| \leq |\text{coker}(\phi)|$
(4) $|\ker(\phi''_n)| \leq |\ker(\phi)| \cdot |\text{coker}(\phi)|$

The first one is obvious. The third one holds because representatives of $\operatorname{coker}(\phi)$ give representatives for $\operatorname{coker}(\phi''_n)$. For the second one, multiply the representatives of $\operatorname{coker}(\phi)$ by $\nu_{n,e}$.
By the Snake lemma there is a long exact sequence

$$0 \to \ker(\phi'_n) \to \ker(\phi) \to \ker(\phi''_n) \to \operatorname{coker}(\phi'_n) \to \operatorname{coker}(\phi) \to \operatorname{coker}(\phi''_n) \to 0.$$

The only nontrivial part is the map $\ker(\phi''_n) \to \operatorname{coker}(\phi'_n)$. Let $x \in \ker(\phi''_n)$. Then there exists $y \in Z$ which maps to $x$. Since $\phi(y)$ maps to 0 in $E/\nu_{n,e}E$ because the diagram is commutative, we must have $\phi(y) \in \nu_{n,e}E$. It can be seen that $\phi(y) \mod \phi'_n(\nu_{n,e}Z)$ depends only on $x$. Then the map $x \mapsto \phi(y)$ is the desired one. It can be checked that this map makes the sequence exact. Now it follows that

$$|\ker(\phi''_n)| \ \leq |\ker(\phi)| \cdot |\operatorname{coker}(\phi'_n)| \leq |\ker(\phi)| \cdot |\operatorname{coker}(\phi)|$$

which is the last inequality.

Now consider $m \geq n \geq 0$. We have the following additional inequalities:

(a) $|\ker(\phi'_n)| \geq |\ker(\phi'_m)|$,
(b) $|\operatorname{coker}(\phi'_n)| \geq |\operatorname{coker}(\phi'_m)|$,
(c) $|\operatorname{coker}(\phi''_n)| \leq |\operatorname{coker}(\phi''_m)|$.

For the first one, we have to observe that $\nu_{m,e} = (\nu_{m,e}/\nu_{n,e})\nu_{n,e}$. Hence $\nu_{m,e}Z \subseteq \nu_{n,e}Z$, so $\ker \phi'_m \subseteq \ker \phi'_n$. For the second one, let $\nu_{m,e}y \in \nu_{m,e}E$. Let $z \in \nu_{n,e}E$ be a representative for $\nu_{n,e}y$ in $\operatorname{coker}(\phi'_n)$. Then

$$\nu_{n,e}y - z = \phi(\nu_{n,e}x) \text{ for some } x \in Z.$$

Now multiply by $\nu_{m,e}/\nu_{n,e}$ to obtain

$$\nu_{m,e}y - \left(\frac{\nu_{m,e}}{\nu_{n,e}}\right) z = \phi(\nu_{m,e}x) = \phi'_m(\nu_{m,e}x).$$

This proves that $\nu_{m,e}/\nu_{n,e}$ times representatives for $\operatorname{coker}(\phi'_n)$ gives representatives for $\operatorname{coker}(\phi'_m)$, which is the second result. The third follows from $\nu_{m,e}E \subseteq \nu_{m,e}E$.

Now by all the inequalities showed up to this moment we can infer that the orders of $\ker \phi'_n$, $\operatorname{coker}(\phi'_n)$ and $\operatorname{coker}(\phi''_n)$ are constant for $n \geq n_0$. It remains to show that $\ker \phi''_n$ is also constant for $n$ sufficiently large, but this follows from the fact that, taking the alternate products of the exact sequence obtained via the snake lemma, we get

$$|\ker \phi'_n| \ |\ker \phi''_n||\operatorname{coker}(\phi)| = |\operatorname{coker}(\phi'_n)||\operatorname{coker}(\phi''_n)||\ker \phi|.$$

This finishes the proof of the lemma. □

*Proof of theorem 3.8.*
All it remains is to verify that $Z_e$ satisfies the hypothesis of lemma 3.15, but $Z_e/\nu_{n,e}Z_e$ is finite because of lemma 3.13 and we obtained the pseudoisomorphism $Z_e \sim E$ by the structure theorem, which at the same time allowed us to see that $E$ satisfies the hypothesis

of proposition 3.14. Thus we have $Z_e \sim E$ with $E$ as in proposition 3.15 and therefore integers $\lambda \geq 0$, $\mu \geq 0$ and $\nu$, and an integer $n_0$ such that $p^{e_n} = |Y_n| = |Y_\infty / Z_e||Z_e/\nu_{n,e}Z_e| = p^c|E/\nu_{n,e}E| = p^{\lambda n + \mu p^n + \nu}$ for all $n > n_0$, where $c$ is a constant, and we have completed the proof of the Iwasawa control theorem. $\square$

# Chapter 4
# The principal conjecture of Iwasawa theory

In this chapter we will continue using the same notation as in chapter 3. In particular, we denoted by $F_\infty/F$ a $\mathbb{Z}_p$-extension of a number field $F$, by $L_\infty$ the maximal unramified $p$-extension of $F_\infty$ and we defined $Y_\infty = \mathrm{Gal}(L_\infty/K_\infty)$.

In chapter 3, we saw that $Y_\infty$ is a finitely generated torsion $\Lambda$-module and that

$$Y_\infty \sim \bigoplus_j \Lambda/(p_j^{k_j}) \oplus \bigoplus_j \Lambda/(f_j^{m_j})$$

and we wrote $\mu = \sum_j k_j$ and $\lambda = \sum_j m_j \deg f_j$. We also saw that that those $\lambda$ and $\mu$ control the growth of the $p$-part of the class number of the $\mathbb{Z}_p$-extension $F_\infty/F$ (theorem 3.8).

In chapter 2, we defined the characteristic ideal of a finitely generated torsion $\Lambda$-module. For $Y_\infty$, this is

$$\mathrm{ch}(Y_\infty) = \left( p^\mu \cdot \prod_j f_j^{m_j} \right).$$

Note that the characteristic ideal $\mathrm{ch}(Y_\infty)$ encodes the constants $\lambda$ and $\mu$ which control the growth of the $p$-part of the class number of the $\mathbb{Z}_p$ extension $F_\infty/F$ according to the Iwasawa control theorem (theorem 3.8). Our goal for the rest of the thesis is to better understand the characteristic ideal in order to know more about the two constants $\lambda$ and $\mu$. In fact, $\mu$ is well understood when $F/\mathbb{Q}$ is abelian. We have the following theorem (the interested reader can find out more about it in [**18**, §7]).

Theorem 4.1 (Ferrero - Washington). *Suppose $F/\mathbb{Q}$ is abelian. Then*

$$\mu(F_\infty/F) = 0.$$

The behaviour of $\lambda$ for totally real fields is also conjectured (see [**4**]):

Conjecture 4.2 (Greenberg). *Suppose that $F$ is totally real. Then*

$$\lambda(F_\infty/F) = 0.$$

The result that will provide us a better understanding of the characteristic ideal is the Iwasawa Main Conjecture (sometimes we will say IMC for short). The aim of this chapter is to state it and to lay out the strategy of proof that is developed in [**2**]. Because of this, in this chapter we will not prove any theorem nor give comprehensive treatments of some concepts. Most of those concepts are worked with more detail in the final chapter.

From now on, we will focus on the particular case $F = \mathbb{Q}(\mu_p)^+$. Since the extension $F/\mathbb{Q}$ is totally real and abelian, by remark 3.3 it has only one $\mathbb{Z}_p$-extension, the cyclotomic $\mathbb{Z}_p$-extension. Using the notation we established in previous chapters and above, we will denote it by $F_\infty/F$, and we will let $L_\infty$ be the maximal abelian $p$-extension of $F_\infty$ that is unramified everywhere. Observe that $F_\infty = \mathbb{Q}(\mu_{p^\infty})^+$, where $\mu_p^\infty$ is the set of all $p$-power roots of unity. We also have that the intermediate field extensions of proposition 3.1 are $F_n = \mathbb{Q}(\zeta_n)^+$.

In this chapter, we will need to consider a larger extension of $F_\infty$. Let $M_\infty$ be the maximal abelian $p$-extension of $F_\infty$ unramified outside the prime above $p$. Denote

$$X_\infty = \mathrm{Gal}(M_\infty/F_\infty).$$

Define $\Delta = \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\mu_p)^+/\mathbb{Q}) = \mathbb{Z}/((p-1)/2)\mathbb{Z}$ and $G = \mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Gamma \times \Delta$, where as in chapter 3 we set $\Gamma = \mathrm{Gal}(F_\infty/F)$. Note that, by lemma 3.6,

$$\Lambda[\Delta] \cong \mathbb{Z}_p[[T]][\Delta] \cong \lim_{\leftarrow} \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})^+/\mathbb{Q}] =: \Lambda(G).$$

Because of this we will write $\mathrm{ch}_G(M) = \mathrm{ch}_\Delta(M)$ for the characteristic ideal defined in definition 2.17. We have the diagram of field extensions and Galois groups of figure 4.1.

Considering the characteristic ideals $\mathrm{ch}_G(X_\infty)$ and $\mathrm{ch}_G(Y_\infty)$ makes sense because of the following result:

PROPOSITION 4.3. *$Y_\infty$ and $X_\infty$ are $\Lambda(G)$-modules.*

*Proof.* It suffices to see that $Y_\infty$ (resp. $X_\infty$) is a $G$-module. Let $g \in G$ and let $\tilde{g} \in \mathrm{Gal}(L_\infty/\mathbb{Q})$ (resp. $\tilde{g} \in \mathrm{Gal}(M_\infty/\mathbb{Q})$) be a lift of $g$. Then define

$$g \cdot y = \tilde{g} y \tilde{g}^{-1}$$

where $y \in Y_\infty$ (resp. $y \in X_\infty$). This action is well defined in both cases since $X_\infty$ and $Y_\infty$ are both abelian. □

REMARK 4.4. In fact, as we will see later in this chapter, we will formulate the main conjecture of Iwasawa theory in terms of the characteristic ideal $\mathrm{ch}_G(X_\infty)$ rather than in terms of $\mathrm{ch}_G(Y_\infty)$, which is the characteristic ideal that has concerned us until now. Using the module $\mathrm{ch}_G(X_\infty)$ is much more convenient in the strategy of proof that we will follow, and the module $\mathrm{ch}_G(Y_\infty)$ can be retrieved from $\mathrm{ch}_G(X_\infty)$, but this will be beyond the scope of this thesis.

The following result allows us to apply the structure theory that we developed in the second chapter to the module $X_\infty$:

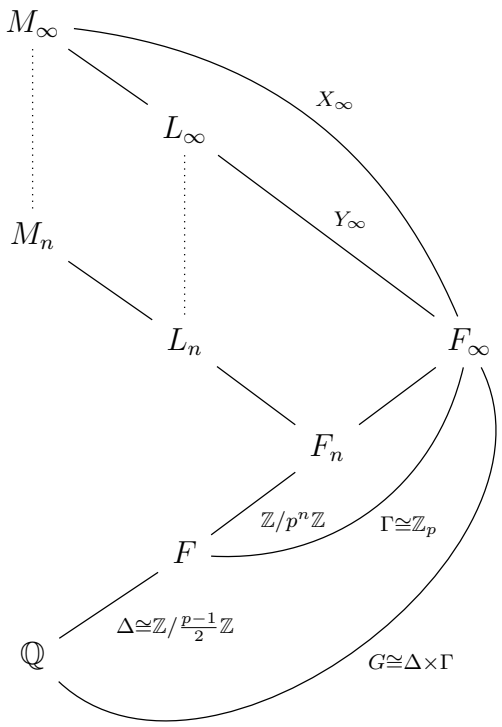


FIG. 4.1. Field extensions defined in chapter 4 and their Galois groups.

PROPOSITION 4.5. *The module $X_\infty$ is a finitely generated torsion $\Lambda(G)$-module.*

One can find the proof of proposition 4.5 in [**18**, §13.5]. Recall that, as we stated in chapter 2, the structure theorem for $\Lambda(G)$-modules (theorem 2.16) gives the following exact sequence for any torsion finitely generated $\Lambda(G)$-module $N$

$$0 \to D' \to \bigoplus_{j=1}^{r} \frac{\Lambda(G)}{g_j \Lambda(G)} \to N \to D \to 0$$

where $g_j$ is a non-zero divisor and $D, D'$ are finite (in fact, one can show that $D'$ is zero). We defined the characteristic ideal of $N$ as $\mathrm{ch}_G(N) = (g_1 \cdots g_r)$.

Another concept that we need to define in order to state the IMC is the $p$-adic analogue of the Riemann zeta function. We need to introduce some new definitions: a *pseudo-measure* $\mu$ is an element $\mu$ of the ring of fractions of $\Lambda(G)$ such that $(g-1)\mu \in \Lambda(G)$ for all $g \in G$. It can be shown (see §5.3) that a pseudo-measure defines a functional

$$\begin{array}{rccc} \mu: & \mathcal{C}(G, \mathbb{C}_p) & \longrightarrow & \mathbb{C}_p \\ & \nu & \longmapsto & \displaystyle\int_G \nu \, \mathrm{d}\mu. \end{array}$$

where $\mathcal{C}(G, \mathbb{C}_p)$ is the $\mathbb{C}_p$-algebra of continuous functions from $G$ to $\mathbb{C}_p$.

We also need to define the *cyclotomic character* $\chi$. It is the character

$$\begin{array}{rccc} \chi: & \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) & \longrightarrow & \mathbb{Z}_p^\times \\ & g & \longmapsto & \chi(g) \end{array}$$

such that $\zeta_n^{\chi(g)} = g(\zeta_n)$ for all $g \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$.

The following key theorem, which we will prove in the next chapter, proves the existence of a $p$-adic analogue of the Riemann zeta function as a pseudo-measure:

THEOREM 4.6. *There exists a unique pseudo-measure $\boldsymbol{\zeta}_p$ on $G$ such that*

$$\int_G \chi(g)^k \, d\boldsymbol{\zeta}_p = (1 - p^{k-1})\boldsymbol{\zeta}(1-k)$$

*for all even integers $k \geq 2$, where $\chi$ is the cyclotomic character and $\boldsymbol{\zeta}$ is the Riemann zeta function.*

The last concept that we have to define that is involved in the IMC is the *augmentation ideal* $I(G)$, which is defined as the kernel of the augmentation homomorphism $\mathrm{aug} : \Lambda(G) \longrightarrow \mathbb{Z}_p$. At a finite level,

$$\mathrm{aug}\left(\sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+/\mathbb{Q})} a_g \cdot g\right) = \sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)^+/\mathbb{Q})} a_g.$$

We will also see that we can interpret $p$-adic measures as elements of the Iwasawa algebra (see proposition 5.17 in the next chapter). Since $\boldsymbol{\zeta}_p$ is a pseudo-measure and $I(G)$ is an ideal of $\Lambda(G)$, $I(G)\boldsymbol{\zeta}_p$ is an ideal of $\Lambda(G)$. Now we are ready for the main conjecture:

THEOREM 4.7 (Main conjecture of Iwasawa Theory). *We have*

$$\mathrm{ch}_G(X_\infty) = I(G)\boldsymbol{\zeta}_p.$$

We will devote the rest of the chapter to lay out the proof strategy of the Main Conjecture based in two more major results. Now for each $n \geq 0$ consider the local field

$$K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+.$$

We will write $U_n^1$ for the group of units of $K_n$ which are $\equiv 1 \pmod{\mathfrak{p}_n}$, where $\mathfrak{p}_n$ is the maximal ideal of the ring of integers of $K_n$. Let $D_n$ be the group of cyclotomic units of $F_n$. Thus $D_n$ is generated by all Galois conjugates of

$$\pm \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}}$$

where $\zeta_n$ denotes a primitive $p^{n+1}$-th root of unity, and $e$ is a primitive root modulo $p$ such that $e^{p-1} \not\equiv 1 \pmod{p^2}$. We define $D_n^1$ to be the subgroup of all elements of $D_n$ which are $\equiv 1 \pmod{\mathfrak{p}_\mathfrak{n}}$. Finally, let

$$C_n^1 = \overline{D}_n^1$$

be the closure of $D_n^1$ in $U_n^1$ with respect to the $\mathfrak{p}_n$-adic topology, and define

$$U_\infty^1 = \varprojlim U_n^1,\ C_\infty^1 = \varprojlim C_n^1$$

where the projective limits are taken with respect to the norm maps. The group $G$ acts continuously on both these $\mathbb{Z}_p$ modules, endowing them with an action of $\Lambda(G)$. We have the following theorem, which we shall call Iwasawa theorem from now on.

THEOREM 4.8 (Iwasawa theorem). *The $\Lambda(G)$-module $U_\infty^1/C_\infty^1$ is canonically isomorphic to $\Lambda(G)/I(G)\boldsymbol{\zeta}_p$ where $\boldsymbol{\zeta}_p$ is the p-adic zeta function, and $I(G)$ is the augmentation ideal.*

We will give a proof of this theorem in the following chapter, but we will need to develop quite a bit of theory to reach it. To continue with our proof strategy for the IMC we will need the following result, which is derived from Class Field Theory (see [**18**, §13.1])

$$\mathrm{Gal}(M_\infty/L_\infty) \cong U_\infty^1/E_\infty^1$$

where

$$E_n^1 = \overline{V}_n^1,\ E_\infty^1 = \varprojlim E_n^1$$

with $V_n^1$ being the group of units of the ring of integers of $F_n$ which are $\cong 1 \pmod{\mathfrak{p}_n}$ and again where the closure is taken with respect to the $p$-adic topology and the projective limit taken with respect to the norm map. Galois theory gives us the exact sequence

$$1 \to \mathrm{Gal}(M_\infty/L_\infty) \to \mathrm{Gal}(M_\infty/F_\infty) \to \mathrm{Gal}(L_\infty/F_\infty) \to 1$$

which gives

$$1 \to E_\infty^1/C_\infty^1 \to U_\infty^1/C_\infty^1 \to X_\infty \to Y_\infty \to 1.$$

Those exact sequences, together with Iwasawa's theory and proposition 2.18, allow us to write

$$\mathrm{ch}_G\left(E_\infty^1/C_\infty^1\right) \cdot \mathrm{ch}_G\left(\Lambda(G)/I(G)\boldsymbol{\zeta}_p\right)^{-1} \cdot \mathrm{ch}_G\left(X_\infty\right) \cdot \mathrm{ch}_G\left(Y_\infty\right)^{-1} = 1.$$

Therefore, assuming Iwasawa's theorem, the following theorem implies the Iwasawa Main Conjecture, as $\mathrm{ch}_G\left(\Lambda(G)/I(G)\boldsymbol{\zeta}_p\right) = I(G)\boldsymbol{\zeta}_p$.

THEOREM 4.9. *We have, using the same notation as above,*

$$\mathrm{ch}_G(Y_\infty) = \mathrm{ch}_G\left(E_\infty^1/C_\infty^1\right).$$

We have thus reduced the proof of the Iwasawa Main Conjecture to the proof of theorem 4.6, theorem 4.8 and theorem 4.9. In the following chapter we will develop the theory that is needed to prove the first and the second ones. The proof of the third one can be found at [**2**, §5-6].

# Chapter 5
# Iwasawa's theorem

In this chapter we intend to develop the theory that will lead to the proof of one of the key ingredients of the proof strategy for the Iwasawa main conjecture that we stated in the previous chapter: the Iwasawa theorem (theorem 4.8). Throughout this chapter our main reference will be [**2**, §2-4]. We will omit the proof of some technical results to focus on developing the theory that will lead us to the proofs of theorems 4.6 and 4.8. The interested reader can find all the details in that reference.

In the first section of this chapter we prove the existence of an exact sequence of power series. Iwasawa's theorem is ultimately a consequence of this exact sequence. To derive Iwasawa's theorem, we need to reinterpret this exact sequence in terms of local units and measures. The link between local units and measures is provided by the Coleman power series, which we present in section 2. Section 3 is devoted to $p$-adic measures. In section 4 we will prove theorem 4.6, which states the existence of a $p$-adic analogue of the Riemann zeta function. We end this thesis by proving Iwasawa's theorem in section 5.

In the previous chapter we worked with the field $F = \mathbb{Q}(\mu_p)^+$ and its unique $\mathbb{Z}_p$-extension, $F_\infty/F$. Working with a totally real field is convenient because it has only a $\mathbb{Z}_p$-extension (see remark 3.3), but for this chapter it will be better for us to consider a $\mathbb{Z}_p$-extension of $\mathcal{F} = \mathbb{Q}(\mu_p)$. Denote by $\mathcal{F}_\infty/\mathcal{F}$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathcal{F}_\infty$ and by $\mathcal{G}$ its Galois group. We also define $\tilde{\Delta} = \mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so that $\mathcal{G} \cong \tilde{\Delta} \times \Gamma$. A diagram containing all those fields and their relations can be found in figure 5.1.

Note that we have

$$\begin{array}{rcl} \Lambda[\tilde{\Delta}] = \mathbb{Z}_p[[T]][\tilde{\Delta}] & \cong & \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})] =: \Lambda(\mathcal{G}) \\ 1+T & \mapsto & \gamma_0. \end{array} \tag{5.2}$$

The natural action of $\mathcal{G}$ on $\Lambda(\mathcal{G})$ tells us that there is an action of $\mathcal{G}$ on $\mathbb{Z}_p[[T]][\tilde{\Delta}]$. The next lemma describes this action on power series in terms of the cyclotomic character that we defined in the previous chapter. With the notation we introduced in this chapter, the cyclotomic character is the character

$$\chi : \mathcal{G} \longrightarrow \mathbb{Z}_p^\times$$

such that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all $\sigma \in \mathcal{G}$ and $\zeta \in \mu_{p^\infty}$.

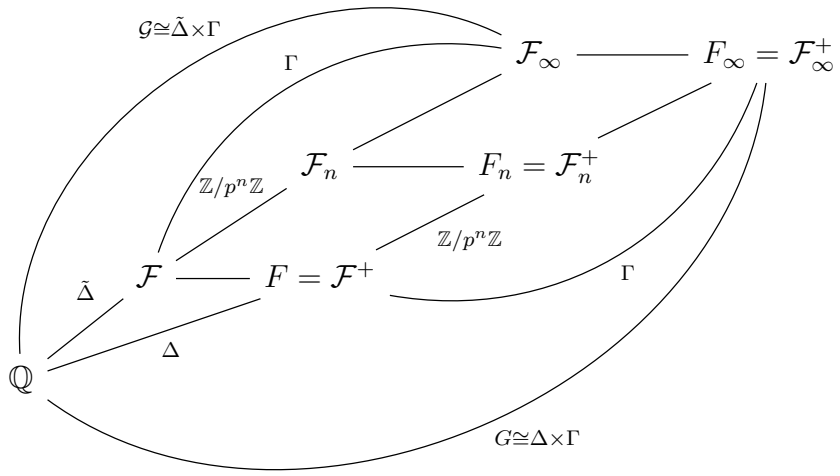


FIG. 5.1. Diagram of field extensions defined in chapter 5 and their Galois groups, and their relation with their maximal totally real fields defined in chapter 4.

LEMMA 5.1. *Let $f\in\mathbb{Z}_p[[T]][\tilde{\Delta}]$ and $\sigma\in\mathcal{G}$. The action on $\mathcal{G}$ on $\mathbb{Z}_p[[T]][\tilde{\Delta}]$ induced by* (5.2) *is given by*

$$(\sigma f)(T)=f((1+T)^{\chi(\sigma)}-1).$$

*Proof.* Note that $(1+T)^{\chi(\sigma)}$ converges in the $(p,T)$-adic topology. Since both actions are continuous, the $\mathcal{G}$-equivariance of (5.2) can be checked on the respective topological generators. Let $\Psi$ denote the isomorphism (5.2). Then, for every $n\in\mathbb{N}$, we have

$$\Psi(\sigma(1+T))(\zeta_n)=\Psi\left((1+T)^{\chi(\sigma)}\right)(\zeta_n)=\zeta_n^{\chi(\sigma)}=\sigma\circ\gamma_0(\zeta_n)=\sigma\Psi(1+T)(\zeta_n).$$

□

## 1. A power series exact sequence

In this section we will develop the theory needed to reach proposition 5.9, which will give us an exact sequence that will be important in our path to the proof of Iwasawa's theorem.

We will start by defining the operator $\varphi$: given $f\in\Lambda$, let

$$\varphi(f)(T):=f((1+T)^p-1).$$

With that definition, it is clear that $\varphi$ is an injective $\mathbb{Z}_p$-algebra endomorphism of $\Lambda$. To check that it is injective, notice that if $h(T)=a_nT^n+\cdots\neq 0$ with $a_n\neq 0$ then $\varphi(h)(T)=$

$p^n a_n T^n + \cdots \neq 0$. Notice that the image of $\varphi$ consists in all the power series $h(T) \in \Lambda$ such that $h(\zeta(1+T)-1) = h(T)$ for all $\zeta \in \mu_p$.

In the following proposition we introduce the operators norm and trace, which will be widely used in this section.

PROPOSITION 5.2. *There exist unique continuous maps*

$$\mathcal{N} : \Lambda \longrightarrow \Lambda, \ \psi : \Lambda \longrightarrow \Lambda$$

*such that*

$$(\varphi \circ \mathcal{N})(f)(T) = \prod_{\zeta \in \mu_p} f(\zeta(1+T)-1),$$

$$(\varphi \circ \psi)(f)(T) = \frac{1}{p} \cdot \sum_{\zeta \in \mu_p} f(\zeta(1+T)-1).$$

*Moreover, $\psi$ is a $\mathbb{Z}_p$-module homomorphism, $\psi \circ \varphi = 1_\Lambda$, and $\mathcal{N}$ preserves products. In particular, $\mathcal{N}$ maps $\Lambda^\times$ to itself.*

The uniquenes of these operators is easy to show and follows from the injectivity of $\varphi$. However, to show its existence is a bit harder and we will need the following lemma:

LEMMA 5.3. *The image of $\varphi$ consists of all power series $h(T)$ in $\Lambda$ satisfying*

$$h(\xi(1+T)-1) = h(T) \text{ for all } \xi \text{ in } \mu_p. \tag{5.3}$$

*Proof.* It is clear that every power series in $\varphi(\Lambda)$ satisfies the condition (5.3). Conversely, let $h(T)$ be any element of $\Lambda$ satisfying (5.3). Since $h(\xi - 1) - h(0) = 0$ for all $\xi$ in $\mu_p$, the Weierstrass preparation theorem (theorem 2.2) shows that

$$h(T) - h(0) = \varphi(T) h_1(T)$$

for some $h_1(T)$ in $\Lambda$. Let $n$ be any positive integer. Assume that we already found $a_0, \ldots, a_{n-1}$ in $\mathbb{Z}_p$ such that

$$h(T) = \sum_{i=0}^{n-1} a_i \varphi(T)^i + \varphi(T)^n h_n(T) \tag{5.4}$$

with $h_n(T)$ in $\Lambda$. Clearly, we again have that $h_n(\xi(1+T)-1) = h_n(T)$, Applying the same procedure as above yields that (5.4) also holds for $n+1$, so the lemma is true by induction. □

*Proof of proposition 5.2.* We will prove first the existence of the operator $\mathcal{N}$. Given $f$ in $\Lambda$, define $h(T) = \prod_{\xi \in \mu_p} f(\xi(1+T)-1)$. Clearly $h(T)$ is in $\Lambda$, and $h(T) = h(\xi(1+T)-1)$ for all $\xi$ in $\mu_p$. By lemma 5.3, $h(T) = \varphi(g(T))$ for some $g(T)$ in $\Lambda$. We can thus take $\mathcal{N}(f) = g$.

The existence of the operator $\psi$ is a bit harder because of the factor $1/p$. We define

$$r(T) = \sum_{\xi \in \mu_p} f(\xi(1+T)-1).$$

Clearly $r(T)$ is in $\Lambda$, and we ust show that

$$r(T) = p \cdot s(T)$$

for some $s(T)$ in $\Lambda$. Let $\mathfrak{p}_0$ be the maximal ideal of the ring of integers of $\mathbb{Q}_p(\mu_p)$. Since for each $\xi$ in $\mu_p$ we have that

$$\xi(1+T) - 1 \equiv T \pmod{\mathfrak{p}_0\Lambda},$$

it follows that $r(T)$ must belong to $p\Lambda$, as claimed. Again, it is clear that $s(\xi(1+T)-1) = s(T)$ for all $\xi$ in $\mu_p$ and therefore $s(T) = \varphi(q(T))$ for some $q(T)$ in $\Lambda$. We can now set $\psi(f) = q$. Now it is clear that $\psi \circ \varphi = 1_\Lambda$ and the proof is complete. □

The operators norm and trace fulfill the following technical properties that will be useful in the next section:

LEMMA 5.4. *Assume $f$ is in $\Lambda$ and let $k \geq 0$ be an integer. If $\varphi(f)(T) \equiv 1 \pmod{p^k\Lambda}$, then $f(T) \equiv 1 \pmod{p^k\Lambda}$.*

*Proof.* Write

$$f(T) - 1 = \left(\sum_{n=0}^{\infty} a_n T^n\right) p^m$$

where not all of the $a_n$ are divisible by $p$ and $m \geq 0$ is an integer. Let $r$ be the smallest integer such that $p \nmid a_r$. We have

$$\varphi(f)(T) - 1 = p^m h(T), \text{ where } h(T) = \sum_{n=0}^{\infty} a_n \varphi(T)^n.$$

Now $\varphi(T) \equiv T^p \pmod{p\Lambda}$, so we have

$$h(T) \equiv a_r T^{pr} + \cdots \pmod{p\Lambda}.$$

Hence, as $p \nmid a_r$, $h(T)$ is not in $p\Lambda$, and our hypothesis implies $m \geq k$. □

LEMMA 5.5. *Assume $f \in \Lambda^\times$. Then $\mathcal{N}(f) \equiv f \pmod{p\Lambda}$. If we assume further that $f \equiv 1 \pmod{p^m\Lambda}$ for some integer $m \geq 1$, then $\mathcal{N}(f) \equiv 1 \pmod{p^{m+1}\Lambda}$.*

*Proof.* Let $\mathfrak{p}_0$ be the maximal ideal of the ring of intege rs of $\mathbb{Q}_p(\mu_p)$. Suppose that $f \equiv 1 \pmod{p^k\Lambda}$ for some integer $k \geq 0$. In other words, if $f(T) = \sum_{n=0}^{\infty} a_n T^n$, we have $a_0 \equiv 1 \pmod{p^k}$ and $a_n \equiv 0 \pmod{p^k}$ for $n \geq 1$. Since for each $\xi$ in $\mu_p$ we have

$$\xi(1+T) - 1 \equiv T \pmod{\mathfrak{p}_0\Lambda},$$

it follows that

$$f(\xi(1+T)-1) \equiv f(T) \pmod{\mathfrak{p}_0 p^k \Lambda}.$$

Thus

$$\varphi(\mathcal{N}(f)) = \prod_{\xi \in \mu_p} f(\xi(1+T)-1) \equiv f(T)^p \pmod{p^{k+1}\Lambda}.$$

If $k \geq 1$, then plainly $f(T)^p \equiv 1 \pmod{p^{k+1}\Lambda}$ and the assertion of the lemma follows from lemma 5.4. If $k = 0$, we note that

$$f(T)^p \equiv f(T^p) \equiv \varphi(f)(T) \pmod{p\Lambda}$$

and again the result follows from lemma 5.4. □

COROLLARY 5.6. *Assume $f$ is in $\Lambda^\times$, and let $k_2 \geq k_1 \geq 0$. Then $\mathcal{N}^{k_2}(f) \equiv \mathcal{N}^{k_1}(f)$ (mod $p^{k_1+1}\Lambda$).*

*Proof.* Note that $\mathcal{N}^{k_2-k_1}(f)/f \equiv 1 \pmod{p\Lambda}$ by lemma 5.5. If we apply $\mathcal{N}^{k_1}$ to both sides we get the corollary from the second assertion of the lemma. □

COROLLARY 5.7. *If $f$ is in $\Lambda^\times$, then $g = \lim_{k\to\infty} \mathcal{N}^k(f)$ exists in $\Lambda^\times$ and $\mathcal{N}(g) = g$.*

*Proof.* The ring $\Lambda$ is complete in the topology defined by the powers of the maximal ideal $\mathfrak{m} = (p, T)$, and the assertion follows from Corollary 5.6. □

The following lemma will also be useful to prove some results:

LEMMA 5.8. *We have $(1 - \varphi)\Lambda = T\Lambda$.*

*Proof.* The inclusion of $(1-\varphi)\Lambda$ in $T\Lambda$ is clear. Conversely, let $h$ be any element of $T\Lambda$. For each $n \geq 0$, define $\omega_n(T) = (1+T)^{p^n} - 1$. This is a distinguished polynomial of degree $p^n$, so by the division lemma part of the Weierstrass preparation theorem (lemma 2.4) we can write

$$h = h_n + \omega_n r_n,$$

where $h_n$ is a polynomial in $\mathbb{Z}_p[T]$ of degree less than $p^n$, and $r_n$ is an element of $\Lambda$. We now define

$$l_n = \sum_{i=0}^{n-1} \varphi^i(h_{n-i}).$$

We have

$$l_{n+1} - \varphi(l_n) = h_{n+1}.$$

Since $h_{n+1}$ converges to $h$ in $\Lambda$, it suffices to show that $l_n$ converges to some $l$ in $\Lambda$, because then we would have $h = (1-\varphi)l$. Now, for $1 \leq k \leq n$, we have

$$\varphi^{n-k}(h) = \varphi^{n-k}(h_k) + \omega_n \varphi^{n-k}(r_k).$$

If we add up these equations for $1 \leq k \leq n$, we obtain the identity

$$\sum_{i=0}^{n} \varphi^i(h) = l_n + \omega_n s_n,$$

for some $s_n$ in $\Lambda$. As $h$ is in $T\Lambda$, it is clear that the sum on the left hand side converges as $n$ tends to infinty. □

Since $\mathcal{N}$ maps $\Lambda^\times$ to itself, it makes sense to define the set of units of $\Lambda$ that are invariant by $\mathcal{N}$:

$$W := \{f \in \Lambda^\times : \mathcal{N}(f) = f\ \}.$$

The subsets of $\Lambda$ that are made up of the power series that are either 0 or invariant upon the application of $\psi$ will also be of interest. We will use the following notation

$$\Lambda^{\psi=0} = \{f \in \Lambda : \psi(f) = 0\},\ \Lambda^{\psi=1} = \{f \in \Lambda : \psi(f) = f\}.$$

PROPOSITION 5.9. *There exists an exact sequence of $\mathcal{G}$-modules*

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \Lambda^{\psi=1} \xrightarrow{\theta} \Lambda^{\psi=0} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

*where $\theta(f) = (1-\varphi)(f)$, and where the map on the left is the natural inclusion, while the map on the right is evaluation at $T = 0$.*

*Proof.* Note that $\theta$ maps $\Lambda^{\psi=1}$ to $\Lambda^{\psi=0}$ because $\psi \circ \varphi = 1_\Lambda$. It is also clear that the image of $\mathbb{Z}_p$ is contained in the kernel of $\theta$, and that the image of $\theta$ is contained in the kernel of the map on the right. The map on the right is surjective, since $1 + T$ belongs to $\Lambda^{\psi=0}$. By lemma 5.8, the ideal $T\Lambda$ is the image of $\theta$.
The only thing remaining is to show exactness at $\Lambda^{\psi=1}$. As remarked earlier, $\mathbb{Z}_p$ lies in the kernel of $\theta$. If $f(T)$ is not in $\mathbb{Z}_p$, it will be of the form

$$f(T) = b_0 + b_r T^r + \cdots, \text{ where } b_r \neq 0,$$

but

$$\varphi(f(T)) = b_0 + p^r b_r T^r + \cdots,$$

so clearly $\varphi(f) \neq f$. The $\mathcal{G}$-equivariance follows from the $\mathcal{G}$-equivariance of the maps $\varphi$, $\mathcal{N}$ and $\psi$, so the proof of the lemma is complete. □

## 2. The Coleman power series

To prove Iwasawa's theorem, we need to reinterpret the exact sequence of the previous section in terms of local units and measures. The key ingredient that allows us to do it is the Coleman power series that we will introduce in this section.

Let $n$ be a natural number, and define $\mathcal{K}_n := \mathbb{Q}_p(\mu_{p^{n+1}})$, where as usual $\mu_{p^{n+1}}$ is the group of the $p^{n+1}$-th roots of unity. Let $\mathcal{U}_n$ be the multiplicative group of units of the ring of integers of $\mathcal{K}_n$. As in the rest of the thesis, $\zeta_n$ will be a generator of $\mu_{p^{n+1}}$, such that $\zeta_n^p = \zeta_{n-1}$. Define

$$\pi_n = \zeta_n - 1.$$

By those definitions, $(\zeta_n)$ is a generator of the free $\mathbb{Z}_p$-module of rank 1 defined by

$$T_p(\mu) = \varprojlim \mu_{p^{n+1}}$$

where the projective limit has been taken with respect to the map consisting in taking the $p$-power. As we saw previously, $\pi_n$ is a local uniformizing parameter for $\mathcal{K}_n$. We may therefore find a power series $f(T) \in \mathbb{Z}_p[[T]] = \Lambda$ such that $f(\pi_n) = z$ for any $z \in \mathcal{U}_n$ (theorem 1.4). It is important to notice that $f(T)$ is not uniquely determined by $z$, so one cannot define properly the derivative of $z$ using the series $f(T)$. A clever way to overcome this problem is to consider all $n$ simultaneously.

If one denotes the norm map from the multiplicative group of $\mathcal{K}_n$ to $\mathcal{K}_m$ by $N_{n,m}$ for $n \geq m$, then $N_{n,n-1}$ maps $\mathcal{U}_n$ to $\mathcal{U}_{n-1}$, allowing us to define $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$, where the projective limit is taken with respect to the norm maps. Then we have the following important theorem:

THEOREM 5.10. *For each $\mathbf{u} = (u_n)$ in $\mathcal{U}_\infty$, there exists a unique $f_{\mathbf{u}}(T) \in \Lambda$ such that $f_{\mathbf{u}}(\pi_n) = u_n$ for all $n \geq 0$. The power series $f_{\mathbf{u}}(T)$ will be called the* Coleman power series.

*Proof.* The uniqueness of the Coleman power series $f_{\mathbf{u}}(T)$ is easy to prove, as it is a consequence of the Weierstrass preparation theorem (theorem 2.2). If we did not have uniqueness, we could build a power series which would have infinitely many zeros, contradicting the uniqueness of the distinguished polynomial of the Weierstrass preparation theorem.

To prove existence, let $\mathbf{u}$ be any element of $\mathcal{U}_\infty$. For each $n \geq 0$, choose $f_n$ in $\Lambda^\times$ such that $f_n(\pi_n) = u_n$, and consider the sequence $\{g_n\}$ in $\Lambda$ where $g_n(T) = \mathcal{N}^n f_{2n}(T)$.

We claim that for all $n \geq 0$, and all $m \geq n$, we have that $g_m(\pi_n) \equiv u_n \pmod{p^{m+1}}$. In particular, $\lim_{m\to\infty} g_m(\pi_n) = u_n$: since $u_{n-1} = N_{n,n-1}(u_n)$, we conclude that $u_{n-1} = (\mathcal{N} f_n)(\pi_{n-1})$. Repeating this $k$ times for $1 \leq k \leq n$, we find

$$u_{n-k} = N_{n,n-k}(f_n(\pi_n)) = (\mathcal{N}^k f_n)(\pi_{n-k}).$$

Now suppose that $m \geq n$. We obtain

$$u_n = (\mathcal{N}^{2m-n} f_{2m})(\pi_n).$$

Using corollary 5.6 we get

$$\mathcal{N}^{2m-n} f_{2m} \equiv \mathcal{N}^m f_{2m} \pmod{p^{m+1}\Lambda}.$$

Evaluating both sides of this congruence at $\pi_n$, we conclude $u_n \equiv g_m(\pi_n) \pmod{p^{m+1}\Lambda}$ so the proof of the claim is finished.

Since $\Lambda$ is compact with respect to its topology, the sequence $\{g_n\}$ has at least one limit point that we denote by $h(T)$. The previous claim shows that $h(T)$ satisfies $h(\pi_n) = u_n$ for all $n \geq 0$, so we can take $h(T)$ to be $f_{\mathbf{u}}(T)$ and complete the proof. □

We now give the explicit computation of the Coleman power series for a particular case:

Example 5.11. Let $a$ and $b$ be non-zero integers relatively prime to $p$, and define

$$\mathbf{u} = (u_n), \text{ where } u_n = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}.$$

The conditions of the theorem hold as $u_n$ is a unit in $\mathcal{U}_n$ and $N_{n,m}(u_n) = u_m$ for $n \geq m$. Consider the power series

$$w_k(T) = \frac{(1+T)^{-k/2} - (1+T)^{k/2}}{T}$$

which is a unit in $\Lambda$ whenever $k$ and $p$ are coprime. Thus the power series

$$f_{\mathbf{u}}(T) = \frac{w_a(T)}{w_b(T)}$$

belongs to $\Lambda$ and satisfies $f_{\mathbf{u}}(\pi_n) = u_n$ for all $n$, proving the existence of the power series of the theorem in this particular case.

Recall that theorem 5.10 gives a map $\mathbf{u} \mapsto f_{\mathbf{u}}(T) : \mathcal{U}_\infty \to W$. This map, in fact, defines an isomorphism, as can be checked easily from the proof of the theorem:

Corollary 5.12. *The map $\mathbf{u} \mapsto f_{\mathbf{u}}(T)$ defines a $\mathcal{G}$-isomorphism from $\mathcal{U}_\infty$ onto $W$.*

With those results we can now continue the work of the previous section in order to reinterpret the exact sequence in terms of local units. We will begin by discussing the relationship between $W$ and $\Lambda^{\psi=1}$. If we denote the formal derivative with respect to $T$ of any power series $f(T) \in \Lambda$ by $f'(T)$, we may define the following operator

$$\Delta(f) := (1+T)\frac{f'(T)}{f(T)}$$

for $f \in \Lambda^\times$. It is clear that the operator $\Delta$ is a group homomorphism from $\Lambda^\times$ to the additive group of $\Lambda$. Further, we have the following result, which we shall not prove here (see [**2**, §2.4]):

THEOREM 5.13. *We have* $\Delta(W) = \Lambda^{\psi=1}$.

We will now introduce a canonical map that will be the key to proving Iwasawa's theorem:

LEMMA 5.14. *For all* $f$ *in* $\Lambda^\times$, *the series*

$$\mathcal{L}(f) := \frac{1}{p}\log\left(\frac{f(T)^p}{\varphi(f)(T)}\right)$$

*lies in* $\Lambda$. *If* $f$ *lies in* $W$, *then* $\mathcal{L}(f)$ *lies in* $\Lambda^{\psi=0}$. *The map* $\mathcal{L} : W \to \Lambda^{\psi=0}$ *thus defined is a* $\mathcal{G}$*-isomorphism, with the* $\mathcal{G}$*-action defined in lemma 5.1.*

*Proof.* For any $f$ in $\Lambda^\times$, we have

$$\varphi(f) \equiv f(T)^p \pmod{p\Lambda}.$$

Hence, writing $g(T) = f(T)^p/\varphi(f)(T)$, it follows that

$$g(T) = 1 + ph(T)$$

for some $h(T)$ in $\Lambda$. We have that $p^{n-1}/n$ lies in $\mathbb{Z}_p$ for all $n = 1, \ldots$, and thus

$$\log(g(T)) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}p^n h(T)^n}{n}$$

converges to an element of $p\Lambda$, proving that $\mathcal{L}$ lies in $\Lambda$. It is clear that $\mathcal{L}$ is a $\mathcal{G}$-isomorphism.

We will now show that $\mathcal{L}(f)$ lies in $\Lambda^{\psi=0}$ when $f$ is in $W$. Since every element of $\Lambda$ can be written as a product of an element in $\mu_{p-1}$ and a power series whose constant term is congruent to 1 modulo $p$, we may assume that the constant term of $f$ is congruent to 1 modulo $p$. Hence the series $\log(f(T))$ is a well-defined element of $\mathbb{Q}_p[[T]]$. Since $f$ is in $W$, we have the equation

$$\varphi(f(T)) = \prod_{\xi \in \mu_p} f(\xi(1+T) - 1).$$

Taking logarithms of both sides of this equation yields

$$\log \varphi(f)(T) = \sum_{\xi \in \mu_p} \log f(\xi(1+T) - 1).$$

Therefore we have that

$$\sum_{\xi \in \mu_p} \mathcal{L}(f)(\xi(1+T) - 1) = 0,$$

which by proposition 5.2 shows that $\mathcal{L}(f)$ belongs to $\Lambda^{\psi=0}$. □

Now let $A$ be the subset of $\Lambda^\times$ defined by

$$A = \{\zeta(1+T)^a : \zeta \in \mu_{p-1}, a \in \mathbb{Z}_p\},$$

and let $D$ be the differential operator on $\Lambda$ defined by $D(f) = (1+T)f'(T)$. We have the following exact sequence:

THEOREM 5.15. *There is a canonical exact sequence of $\mathcal{G}$-modules*

$$0 \longrightarrow A \longrightarrow W \xrightarrow{\mathcal{L}} \Lambda^{\psi=0} \xrightarrow{\alpha} \mathbb{Z}_p \longrightarrow 0$$

*where $\alpha$ is given by $\alpha(f) = (Df)(0)$.*

*Proof.* It is clear that $A \subset \ker(\mathcal{L})$. To prove the converse, note that if $f(T)$ is an element of $\Lambda$ with $f(0) \equiv 1 \pmod p$ and $\log f(T) = 0$, then $f(T) = 1$. Indeed, we can write $f(T) = bg(T)$ with $b \equiv 1 \pmod p$ and $g(T)$ of the form

$$g(T) = 1 + c_r T^r + \cdots$$

where $r \geq 1$ and $c_r \neq 0$. Now

$$\log g(T) = c_r T^r + \cdots .$$

But $\log f(T) = 0$ gives

$$0 = \log b + \log g(T),$$

from where we deduce that $b = 1$ and $\log g(T) = 0$, contradicting the hypothesis that $c_r = 0$.

Suppose now that $f(T)$ is any element of $\ker(\mathcal{L})$. Multiplying it by a suitable element of $\mu_{p-1}$, we may suppose that $f(0) \equiv 1 \pmod p$, and the same is true for $h(T) = f(T)^p/\varphi(f(T))$. But then, we have again that $\mathcal{L}(f) = 0$ yields $h(T) = 1$. By corollary 5.12, there exists a unique $\mathbf{u} = (u_n)$ in $\mathcal{U}_\infty$ such that $f = f_{\mathbf{u}}$ and hence we have

$$f_{\mathbf{u}}((1+T)^p - 1) = f_{\mathbf{u}}(T)^p.$$

This implies that $u_n^p = u_{n-1}$ for all $n \geq 1$ and that $f_{\mathbf{u}}(0)$ is in $\mu_{p-1}$. But $f_{\mathbf{u}}(0) = 1$ since $f_{\mathbf{u}} \equiv 1 \pmod p$ and so $(u_n) \in T_p(\mu)$. Thus there exists $a$in $\mathbb{Z}_p$, such that $\mathbf{u} = (\zeta_n)^a$, whence $f(T) = (1+T)^a$. Thus $\ker(\mathcal{L}) = A$.

It is clear that $\alpha \circ \mathcal{L} = 0$, and the surjectivity of $\alpha$ follows from noting that $\psi(1+T) = 0$ and that $\alpha(1+T) = 1$. It only remains to prove that $\ker(\alpha) \subset \mathrm{Im}(\mathcal{L})$. This is the delicate part of the proof. We have the commutative diagram

$$\begin{array}{ccc} W & \xrightarrow{\mathcal{L}} & \Lambda^{\psi=0} \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle D} \\ \Lambda^{\psi=1} & \xrightarrow{\theta} & \Lambda^{\psi=0} \end{array}$$

where we recall that $\theta(f) = (1-\varphi)(f)$.

First of all, $D$ is clearly injective on $\Lambda^{\psi=0}$. Suppose $f$ is any element of $\Lambda^{\psi=0}$ with $\alpha(f) = 0$. Define $g = Df$ so that $g$ is in $T\Lambda$ by the definition of $\alpha$. Lemma 5.8 shows that there exists $h$ in $\Lambda^{\psi=1}$ with $\theta(h) = g$. But, by theorem 5.13 we have that $\Delta$ is surjective, so we can

conclude that there exists $w$ in $W$ with $\Delta(w) = h$. By construction and the commutativity of the diagram, we have

$$g = Df = D\mathcal{L}(w).$$

Hence $f = \mathcal{L}(w)$ by injectivity of $D$, and $f$ belongs to the image of $\mathcal{L}$ and the proof is complete. □

By joining the results of proposition 5.9 and theorem 5.15 we get the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & W & \xrightarrow{\mathcal{L}} & \Lambda^{\psi=0} & \xrightarrow{\alpha} & \mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \zeta(1+T)^a \mapsto a} & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \Lambda^{\psi=1} & \xrightarrow{\theta} & \Lambda^{\psi=0} & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0 \end{array} \tag{5.5}$$

## 3. $p$-adic measures

For this section, $\mathfrak{G}$ will be any profinite abelian group, written multiplicatively, and $\mathfrak{T}_{\mathfrak{G}}$ will be the set of open subgroups of $\mathfrak{G}$. We can define the Iwasawa algebra of $\mathfrak{G}$ in the same fashion as we did with the groups $G$ and $\mathcal{G}$, i.e.,

$$\Lambda(\mathfrak{G}) := \lim_{\leftarrow} \mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}],$$

where $\mathfrak{H}$ runs over $\mathfrak{T}_{\mathfrak{G}}$. Let $\mathbb{C}_p$ be the completion of the algebraic closure of the field of $p$-adic numbers $\mathbb{Q}_p$, and write $|\cdot|_p$ for its $p$-adic valuation. Let $\mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$ be the $\mathbb{C}_p$-algebra of all continuous functions from $\mathfrak{G}$ to $\mathbb{C}_p$. We can define a norm on $\mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$ by

$$\|f\| := \sup_{g \in \mathfrak{G}} |f(g)|_p,$$

thus making $\mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$ a $\mathbb{C}_p$-Banach space. We can now introduce $p$-adic measures:

Definition 5.16 ($p$-adic measure). *A $p$-adic measure on $\mathfrak{G}$ is a linear functional*

$$M : \mathcal{C}(\mathfrak{G}, \mathbb{C}_p) \longrightarrow \mathbb{C}_p$$

*satisfying that*

- $|M(f)|_p \leq \|f\|$, *where $\|\cdot\|$ denotes the supremum norm,*
- $M(f) \in \mathbb{Q}_p$ *if* $f \in \mathcal{C}(\mathfrak{G}, \mathbb{Q}_p)$.

Our objective will be to prove the fact that the elements of the Iwasawa algebra $\Lambda(\mathfrak{G})$ define integral $p$-adic measures on $\mathfrak{G}$. It is clear the set of $p$-adic measures $\mathrm{Meas}_p(\mathfrak{G})$ is endowed with a structure of $\mathbb{Z}_p$-module.

**3.1. Integrals and pseudo-measures.** We now want to integrate any continuous $\mathbb{C}_p$-valued function on $\mathfrak{G}$ against an element $\lambda$ of $\Lambda(\mathfrak{G})$. We will begin by considering only locally constant functions. We say that a function $f \in \mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$ is *locally constant* if there exists an open subgroup $\mathfrak{H}$ such that $f$ is constant modulo $\mathfrak{H}$, i.e., it gives a function $\mathfrak{G}/\mathfrak{H}$ to $\mathbb{C}_p$. We write $\mathrm{Step}(\mathfrak{G})$ for the sub-algebra of locally constant functions. This sub-algebra is everywhere dense. Suppose that $f \in \mathrm{Step}(\mathfrak{G})$ is locally constant modulo the subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Write $\lambda_{\mathfrak{H}}$ for the image of $\lambda$ in $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$, this is

$$\lambda_{\mathfrak{H}} = \sum_{x \in \mathfrak{G}/\mathfrak{H}} c_{\mathfrak{H}}(x) x, \tag{5.6}$$

where the $c_{\mathfrak{H}}(x)$ lie in $\mathbb{Z}_p$. Now define

$$\int_{\mathfrak{G}} f \, d\lambda = \sum_{x \in \mathfrak{G}/\mathfrak{H}} c_{\mathfrak{H}}(x) f(x).$$

It is easy to see that the value of the integral is independent of $\mathfrak{H}$. We also have (since the $c_{\mathfrak{H}}(x)$ lie in $\mathbb{Z}_p$)

$$\left| \int_{\mathfrak{G}} f \, d\lambda \right|_p \leq \|f\|. \tag{5.7}$$

Furthermore, if $\varepsilon_x$ denotes the characteristic function of the coset x in $\mathfrak{G}/\mathfrak{H}$, then we have

$$\int_{\mathfrak{G}} \varepsilon_x \, d\lambda = c_{\mathfrak{H}}(x) \tag{5.8}$$

We will now consider any continuous $\mathbb{C}_p$-valued function $f$ on $\mathfrak{G}$. We can choose a sequence $\{f_n\}$ in $\mathrm{Step}(\mathfrak{G})$ which converges to $f$. It is easy to see from (5.7) that the sequence of integrals $\left\{\int_{\mathfrak{G}} f_n \, d\lambda\right\}$ is a Cauchy sequence, and hence converges in $\mathbb{C}_p$. Therefore, we can define the integral as

$$\int_{\mathfrak{G}} f \, d\lambda = \lim_{n \to \infty} \int_{\mathfrak{G}} f_n \, d\lambda.$$

Now, if we write $M_\lambda(f) := \int_{\mathfrak{G}} f \, d\lambda$, we get a linear functional on $\mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$ satisfying

$$|M_\lambda(f)|_p \leq \|f\|. \tag{5.9}$$

We have therefore concluded the definition of the integral of a continuous $\mathbb{C}_p$-valued function on $\mathfrak{G}$ against an element $\lambda$ of $\Lambda(\mathfrak{G})$, so are ready to prove the relation between $p$-adic measures and elements of the Iwasawa algebra. In the following proposition we will prove that $p$-adic measures are of the form $M_\lambda$ for $\lambda$ in $\Lambda(\mathfrak{G})$. Therefore, it makes sense to endow the set of $p$-adic measures $\mathrm{Meas}_p(\mathfrak{G})$ with a structure of $\mathbb{Z}_p$-algebra by defining the convolution of two measures:

$$\int_{\mathfrak{G}} f(x) \, d(\lambda_1 * \lambda_2)(x) = \int_{\mathfrak{G}} \left( \int_{\mathfrak{G}} f(x \cdot y) \, d\lambda_1(x) \right) d\lambda_2(y).$$

Proposition 5.17. *There is an isomorphism*

$$\Lambda(\mathfrak{G}) \cong \mathrm{Meas}_p(\mathfrak{G})$$

*of $\mathbb{Z}_p$-algebras, given by sending $\lambda$ to $M_\lambda$.*

*Proof.* We can see from (5.8) that if $M_{\lambda_1} = M_{\lambda_2}$ then $\lambda_1 = \lambda_2$. Further, $M_\lambda(f)$ belongs to $\mathbb{Q}_p$ when $f$ takes values in $\mathbb{Q}_p$. Therefore the functionals $M_\lambda$ we defined are indeed $p$-adic measures. Conversely, we can note that every linear functional $L$ on $\mathcal{C}(\mathfrak{G}, \mathbb{Q}_p)$ satisfying $|L(f)|_p \leq \|f\|$ for all continuous $f$ and such that $L(f)$ belongs to $\mathbb{Q}_p$ when $f$ takes values in $\mathbb{Q}_p$ must be of the form $L = M_\lambda$ for some unique $\lambda$ in the Iwasawa algebra $\Lambda(\mathfrak{G})$. Let us show how one can find the element $\lambda$. For every open subgroup $\mathfrak{H}$ of $\mathfrak{G}$ and each coset $x$ of $\mathfrak{G}/\mathfrak{H}$, we put $c_{\mathfrak{H}}(x) = L(\varepsilon_x)$ where $\varepsilon_x$ is the characteristic function of $x$, and we define $\lambda_{\mathfrak{H}}$ as in the formula (5.6). These elements are clearly compatible and thus they give an element of the Iwasawa algebra.

To see that the map is an isomorphism of $\mathbb{Z}_p$-algebras, we need to see that

$$M_{\lambda_1 \cdot \lambda_2}(f) = \int_{\mathfrak{G}} \left( \int_{\mathfrak{G}} f(x \cdot y)\, d\lambda_1(x) \right) d\lambda_2(y) \tag{5.10}$$

for every $f \in \mathcal{C}(\mathfrak{G}, \mathbb{C}_p)$. By continuity, it is enough to check (5.10) for locally constant functions. Suppose that $f$ is constant modulo $\mathfrak{H}$. Let $\lambda_{1,\mathfrak{H}}$ (resp. $\lambda_{2,\mathfrak{H}}$) denote the image of $\lambda_1$ (resp. $\lambda_2$) in $\mathbb{Z}_p[\mathfrak{G}/\mathfrak{H}]$, say

$$\lambda_{1,\mathfrak{H}} = \sum_{x \in \mathfrak{G}/\mathfrak{H}} c_{1,\mathfrak{H}}(x) \cdot x,\ \lambda_{2,\mathfrak{H}} = \sum_{y \in \mathfrak{G}/\mathfrak{H}} c_{2,\mathfrak{H}}(y) \cdot y$$

where all the $c_{1,\mathfrak{H}}$ and $c_{2,\mathfrak{H}}$ are in $\mathbb{Z}_p$. The left hand side of (5.10) is

$$\sum_{y \in \mathfrak{G}/\mathfrak{H}} \left( \sum_{x \in \mathfrak{G}/\mathfrak{H}} f(x \cdot y) \cdot c_{1,\mathfrak{H}}(x) \right) c_{2,\mathfrak{H}}(y).$$

But this clearly coincides with the right hand side of (5.10) since $M_{\lambda_1 \cdot \lambda_2} = M_{\lambda_{1,\mathfrak{H}} \cdot \lambda_{2,\mathfrak{H}}}$ and

$$\lambda_{1,\mathfrak{H}} \cdot \lambda_{2,\mathfrak{H}} = \sum_{x \in \mathfrak{G}/\mathfrak{H}} \sum_{y \in \mathfrak{G}/\mathfrak{H}} c_{1,\mathfrak{H}}(x) c_{2,\mathfrak{H}}(y) x \cdot y.$$

□

This proposition allows us to think of $p$-adic measures both as linear functionals and as elements of the Iwasawa algebra, at our convenience.

We now give a couple of additional properties of the integral over $\mathfrak{G}$.

- If $\lambda = g \in \mathfrak{G}$, then $dg$ is the Dirac measure:
$$\int_{\mathfrak{G}} f\, dg = f(g).$$
- If $\nu : \mathfrak{G} \longrightarrow \mathbb{C}_p^\times$ is a continuous group homomorphism, we can extend $\nu$ to a continuous algebra homomorphism
$$\begin{array}{rccc} \nu : & \Lambda(\mathfrak{G}) & \longrightarrow & \mathbb{C}_p \\ & \lambda & \longmapsto & v(\lambda) = \displaystyle\int_{\mathfrak{G}} \nu\, d\lambda. \end{array}$$

To take into account the fact that the $p$-adic analogue of the complex Riemann zeta function also has a pole, we introduce the notion of a $p$-adic pseudo-measure on $\mathfrak{G}$. Let $Q(\mathfrak{G})$ be the total ring of fractions of $\Lambda(\mathfrak{G})$, i.e., $Q(\mathfrak{G}) = \{\alpha/\beta \mid \alpha, \beta \in \Lambda(\mathfrak{G}),\ \beta \text{ non-zero divisor}\}$.

DEFINITION 5.18 (Pseudo-measure). *We say that an element $\lambda$ of the ring of fractions $Q(\mathfrak{G})$ is a* pseudo-measure *on $\mathfrak{G}$ if $(g-1)\lambda$ is in $\Lambda(\mathfrak{G})$ for all $g$ in $\mathfrak{G}$.*

Suppose that $\lambda$ is a pseudo-measure on $\mathfrak{G}$ and let $\nu$ be a homomorphism from $\mathfrak{G}$ to $\mathbb{C}_p^\times$ which is not identically one. We can define

$$\int_{\mathfrak{G}} \nu \, d\lambda = \frac{\int_{\mathfrak{G}} \nu \, d((g-1)\lambda)}{\nu(g) - 1},$$

where $g$ is any element of $\mathfrak{G}$ with $\nu(g) \neq 1$. This is idependent of the choice of $g$ because as we stated earlier $\nu$ extends to a ring homomorphism from $\Lambda(\mathfrak{G})$ to $\mathbb{C}_p$.

**3.2. The Mahler transform.** We now revisit the relation between the ring $\Lambda = \mathbb{Z}_p[[T]]$ and the Iwasawa algebra $\Lambda(\mathbb{Z}_p) \cong \Lambda(\Gamma)$, where $\Gamma = \mathrm{Gal}(\mathcal{F}_\infty/\mathcal{F})$ (compare with lemma 3.6). We now present a theorem due to Mahler [**9**] that will be of critical importance for this task. Notice that as usual, we set $\binom{x}{0} = 1$ and

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \text{ for } n \geq 1.$$

THEOREM 5.19. *Let $f : \mathbb{Z}_p \longrightarrow \mathbb{C}_p$ be any continuous function. Then $f$ can be written uniquely in the form*

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \tag{5.11}$$

*where $a_n \in \mathbb{C}_p$ tends to zero as $n \to \infty$.*

It is easy to notice that the coefficients $a_n$ are given by $a_n = (\nabla^n f)(0)$ where $\nabla f(x) = f(x+1) - f(x)$. Since $\left|\binom{x}{n}\right|_p \leq 1$ for all $x$ in $\mathbb{Z}_p$, it follows that $\|f\| = \sup |a_n|_p$. If $\lambda$ is an element of $\Lambda(\mathbb{Z}_p)$, we can deduce from (5.9) that

$$c_n(\lambda) = \int_{\mathbb{Z}_p} \binom{x}{n} d\lambda \text{ for } n \geq 0 \tag{5.12}$$

lies in $\mathbb{Z}_p$.

DEFINITION 5.20 (Mahler transform). *The* Mahler transform $\mathcal{M} : \Lambda(\mathbb{Z}_p) \longrightarrow \Lambda$ *is defined as*

$$\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} c_n(\lambda) T^n,$$

*where $c_n(\lambda)$ is defined as in* (5.12) *for $\lambda$ in $\Lambda(\mathbb{Z}_p)$.*

THEOREM 5.21. *The Mahler transform is an isomorphism of $\mathbb{Z}_p$-algebras.*

*Proof.* It is clear from theorem 5.19 that $\mathcal{M}$ is injective and that it is a $\mathbb{Z}_p$-module homomorphism. To see that is bijective, we construct an inverse $\Upsilon : \Lambda \longrightarrow \Lambda(\mathbb{Z}_p)$ as follows. Let $g(T) = \sum_{n=0}^{\infty} c_n T^n$ be any element of $\Lambda$. Then we can define a linear functional $L$ on $C(\mathbb{Z}_p, \mathbb{C}_p)$ by

$$L(f) = \sum_{n=0}^{\infty} a_n c_n,$$

where $f$ has Mahler expansion as in (5.11). The series on the right converges as $a_n$ tends to zero as $n \to \infty$. Also, since $c_n \in \mathbb{Z}_p$, it is clear that $|L(f)|_p \leq \|f\|$ for all $f$. Therefore there exists $\lambda$ in $\Lambda(\mathbb{Z}_p)$ such that $L = M_\lambda$ and we define $\Upsilon(g(T)) = \lambda$. Clearly, $\Upsilon$ is an inverse of $\mathcal{M}$. □

As we noticed before, we already proved that there existed a isomorphism between the $\mathbb{Z}_p$-algebras $\Lambda$ and $\Lambda(\Gamma)$ in lemma 3.6. In this case what we are doing is to get a explicit isomorphism when we fix the topological generator $\gamma_0$ of $\Gamma$ to be 1. We have following lemmas regarding the Mahler transform $\mathcal{M}$ and its inverse $\Upsilon$.

LEMMA 5.22. *We have that $\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$, and thus $\mathcal{M} : \Lambda(\mathbb{Z}_p) \longrightarrow \Lambda$ is the unique isomorphism of topological $\mathbb{Z}_p$-algebras which sends the topological generator $1_{\mathbb{Z}_p}$ to $1 + T$.*

*Proof.* The first assertion follows from the fact that

$$\mathcal{M}(1_{\mathbb{Z}_p}) = \sum_{n=0}^{\infty} c_n(1_{\mathbb{Z}_p}) T^n$$

with

$$c_n(1_{\mathbb{Z}_p}) = \int_{\mathbb{Z}_p} \binom{x}{n} d1_{\mathbb{Z}_p} = \binom{1}{n}.$$

The second follows from the fact that for each choice of a topological generator $\gamma$ of $\mathbb{Z}_p$ there is a unique topological isomorphism of $\mathbb{Z}_p$-algebras which maps $\gamma$ to $1 + T$ (see [**13**]). □

LEMMA 5.23. *For all $g$ in $\Lambda$, and all integers $k \geq 0$, we have the integral*

$$\int_{\mathbb{Z}_p} x^k \, d(\Upsilon(g(T))) = (D^k g(T))_{T=0}$$

*where $D = (1 + T)\frac{d}{dT}$.*

*Proof.* Fix $g(T) = \sum_{n=0}^{\infty} c_n T^n$ in $\Lambda$ and consider the linear functional $L$ on $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ defined by

$$L(f) = \int_{\mathbb{Z}_p} x f(x) \, d\Upsilon(g(T)).$$

We clearly have that $|L(f)|_p \leq \|f\|$, so $L = M_\lambda$ for some $\lambda$ in $\Lambda(\mathbb{Z}_p)$, so we obtain

$$\int_{\mathbb{Z}_p} x f(x) \, d\Upsilon(g(T)) = \int_{\mathbb{Z}_p} f(x) \, d\lambda. \tag{5.13}$$

We now claim that

$$\mathcal{M}(\lambda) = Dg(T). \tag{5.14}$$

Note that

$$Dg(T) = \sum_{n=0}^{\infty} (nc_n + (n+1)c_{n+1})T^n$$

and that, by definition, $\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} e_n T^n$ with

$$e_n = \int_{\mathbb{Z}_p} x \binom{x}{n} \, d\Upsilon(g(T)).$$

We now apply the identity

$$x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n},$$

valid for $n \geq 0$, to get $e_n = nc_n + (n+1)c_{n+1}$ for all $n \geq 0$, proving our claim.

Now we have

$$\int_{\mathbb{Z}_p} d\Upsilon(h(T)) = h(0),$$

for all $h(T)$ in $\Lambda$, so the assertion of the lemma is equivalent to

$$\int_{\mathbb{Z}_p} x^k \, d\Upsilon(g(T)) = \int_{\mathbb{Z}_p} d\Upsilon(D^k g(T))$$

for $k \geq 0$. By induction, we have

$$\int_{\mathbb{Z}_p} d\Upsilon(D^k g(T)) = \int_{\mathbb{Z}_p} x^{k-1} \, d\Upsilon(Dg(T))$$

but by (5.13) and (5.13) it is clear that this equals

$$\int_{\mathbb{Z}_p} d\Upsilon(D^k g(T))$$

and we are done. □

**3.3. Restriction of measures.** Since as a multiplicative group $\mathbb{Z}_p^\times$ is not a subgroup of the additive group $\mathbb{Z}_p$, it is surprising that we can canonically identify $\Lambda(\mathbb{Z}_p^\times)$ with a subset of $\Lambda(\mathbb{Z}_p)$. We want to explain this identification in terms of power series.

Let $\varepsilon$ be the characteristic function of $\mathbb{Z}_p^\times$ in $\mathbb{Z}_p$. It is continuous because $\mathbb{Z}_p^\times$ is open and closed in $\mathbb{Z}_p$. Given $\lambda$ in $\Lambda(\mathbb{Z}_p)$, we can define a function $L$ on $C(\mathbb{Z}_p, \mathbb{C}_p)$ by

$$L(f) = \int_{\mathbb{Z}_p} f\varepsilon \, d\lambda,$$

and clearly $|L(f)|_p \leq \|f\|$. Hence $L = M_{\#(\lambda)}$ for a unique $\#(\lambda)$, where $M_{\#(\lambda)}$ is defined as in section 3.1. In order to interpret this operation in terms of power series, we define the operator $\mathcal{S} : \Lambda \longrightarrow \Lambda$ by

$$\mathcal{S}(g(T)) = g(T) - \frac{1}{p} \sum_{\zeta \in \mu_p} g(\zeta(1+T) - 1)).$$

This definition reminds us the form of the map $\psi$ defined in proposition 5.2, stated earlier in this chapter. The relation is the following one:

LEMMA 5.24. *For all $\lambda$ in $\Lambda(\mathbb{Z}_p)$, we have $\mathcal{S}(\mathcal{M}(\lambda)) = \mathcal{M}(\#(\lambda))$. In particular, $\#(\lambda) = \lambda$ if and only if $\mathcal{S}(\mathcal{M}(\lambda)) = \mathcal{M}(\lambda)$, or equivalently if and only if $\mathcal{M}(\lambda)$ belongs to $\Lambda^{\psi=0}$.*

*Proof.* For each $n \geq 0$, let

$$\mathrm{pr}_n : \Lambda(\mathbb{Z}_p) \longrightarrow \mathbb{Z}_p[\mathbb{Z}_p/p^n\mathbb{Z}_p]$$

be the natural map. Suppose

$$\mathrm{pr}_n(\lambda) = \sum_{k=0}^{p^n-1} e_n(k)(k + p^n\mathbb{Z}_p) \tag{5.15}$$

with the $e_n(k)$ in $\mathbb{Z}_p$. Now by (5.8) we have

$$e_n(k) = \int_{\mathbb{Z}_p} \varepsilon_{k+p^n\mathbb{Z}_p}\, d\lambda,$$

where $\varepsilon_{k+p^n\mathbb{Z}_p}$ denotes the characteristic function of the subset $k + p^n\mathbb{Z}_p$. We can now see that $\#(\lambda)$ is the unique element of $\Lambda(\mathbb{Z}_p)$ defined by

$$\mathrm{pr}_n(\#(\lambda)) = \sum_{\substack{k=0 \\ (k,p)=1}}^{p^n-1} e_n(k)(k + p^n\mathbb{Z}_p).$$

Weierstrass preparation theorem (theorem 2.2) shows that

$$\mathbb{Z}_p[T]/\omega_n\mathbb{Z}_p[T] \cong \Lambda/\omega_n\Lambda,$$

where $\omega_n(T) = (1+T)^{p^n} - 1$. Now as $\Lambda = \lim_{\leftarrow} \Lambda/\omega_n\Lambda$ we obtain natural maps

$$\mathrm{pr}'_n : \Lambda \longrightarrow \mathbb{Z}_p[T]/\omega_n\mathbb{Z}_p[T].$$

Since lemma 5.22 tells us that $\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$, it follows that

$$\mathrm{pr}'_n(\mathcal{M}(\lambda)) = \sum_{k=0}^{p^n-1} e_n(k)(1+T)^k \pmod{\omega_n\mathbb{Z}_p[T]}$$

and that

$$\mathrm{pr}'_n(\mathcal{M}(\lambda)) = \sum_{\substack{k=0 \\ (k,p)=1}}^{p^n-1} e_n(k)(1+T)^k \pmod{\omega_n\mathbb{Z}_p[T]}$$

for all $n \geq 0$. But now

$$\mathcal{S}\left(\sum_{k=0}^{p^n-1} e_n(k)(1+T)^k\right) = \sum_{\substack{k=0 \\ (k,p)=1}}^{p^n-1} e_n(k)(1+T)^k,$$

so it is clear that $\mathcal{S}(\mathcal{M}(\lambda)) = \mathcal{M}(\#(\lambda))$. The final assertion is clear from the definition of $\psi$ in proposition 5.2. □

Now we can define a natural inclusion

$$i : \Lambda(\mathbb{Z}_p^\times) \to \Lambda(\mathbb{Z}_p)$$

by the formula

$$\int_{\mathbb{Z}_p} f\, d(i(\eta)) = \int_{\mathbb{Z}_p^\times} f|_{\mathbb{Z}_p^\times}\, d\eta,$$

where $f$ runs over all continuous $\mathbb{C}_p$-valued functions and $f|_{\mathbb{Z}_p^\times}$ denotes the restriction to $\mathbb{Z}_p^\times$. We have the following important lemma regarding the image by the Mahler transform of the identification of $\Lambda(\mathbb{Z}_p^\times)$ in $\Lambda(\mathbb{Z}_p)$, which turns out to be exactly $\Lambda^{\psi=0}$.

LEMMA 5.25. *We have that* $i(\Lambda(\mathbb{Z}_p^\times)) = \{\lambda \in \Lambda(\mathbb{Z}_p) \mid \#(\lambda) = \lambda\}$. *In particular,* $\mathcal{M}(i(\Lambda(\mathbb{Z}_p^\times))) = \Lambda^{\psi=0}$.

*Proof.* Clearly the image of $i$ is contained in the set on the right. Conversely, let $\lambda$ in $\Lambda(\mathbb{Z}_p)$ be such that $\#(\lambda) = \lambda$. We can now obtain an element $\eta$ in $\Lambda(\mathbb{Z}_p^\times)$ by specifying that

$$\int_{\mathbb{Z}_p^\times} h\, d\eta = \int_{\mathbb{Z}_p} \tilde{h}\, d\lambda,$$

where $h$ is any continuous $\mathbb{C}_p$-valued function on $\mathbb{Z}_p^\times$ and $\tilde{h}$ denotes its extension by zero to $\mathbb{Z}_p$. Now clearly $i(\eta) = \lambda$ because $\#(\lambda) = \lambda$ and we are done. □

For the rest of the section, we will supress the map $i$ and we will identify $\Lambda(\mathbb{Z}_p^\times)$ with its image by the identification map.

**3.4. The fundamental exact sequence.** Earlier this chapter we obtained a commutative diagram using the exact sequences given by proposition 5.9 and theorem 5.15. We want to combine the above interpretation of $\Lambda(\mathbb{Z}_p^\times)$ with those results to build the fundamental exact sequence that we will need to prove Iwasawa's theorem.

We will consider the action of $\mathcal{G}$ on $\Lambda(\mathbb{Z}_p)$ defined by

$$g \cdot (a_{\mathbb{Z}_p}) = (\chi(g) \cdot a)_{\mathbb{Z}_p}, \quad (a \in \mathbb{Z}_p),$$

where we write $a_{\mathbb{Z}_p}$ to stress that we are viewing $a$ as an element of the group $\mathbb{Z}_p$ in the Iwasawa algebra $\Lambda(\mathbb{Z}_p)$. By linearity and continuity, this action extends to an action of $\mathcal{G}$ on $\Lambda(\mathbb{Z}_p)$. Moreover, since $\mathcal{M}(1_{\mathbb{Z}_p}) = 1 + T$, it is clear that $\mathcal{M}$ is a $\mathcal{G}$-isomorphism from $\Lambda(\mathbb{Z}_p)$ to $\Lambda$ when $\Lambda$ is endowed with the $\mathcal{G}$-action given by

$$(\sigma f)(T) = f((1+T)^{\chi(\sigma)} - 1)$$

for $f \in \Lambda$. Finally we note that there is a canonical $\mathcal{G}$-isomorphism

$$\tilde{\chi} : \Lambda(\mathcal{G}) \cong \Lambda(\mathbb{Z}_p^\times) \tag{5.16}$$

induced by the isomorphism $\chi : \mathcal{G} \cong \mathbb{Z}_p^\times$ given by the cyclotomic character. Let

$$\widetilde{\mathcal{M}} : \Lambda(\mathcal{G}) \cong \Lambda^{\psi=0} \tag{5.17}$$

be the $\mathcal{G}$-isomorphism defined by $\widetilde{\mathcal{M}} = \mathcal{M} \circ \tilde{\chi}$. Recall that $\mathcal{U}_\infty$ denotes the projective limit of the local units with respect to the norm maps in the cyclotomic tower endowed with its natural acton of $\mathcal{G}$. Now define

$$\widetilde{\mathcal{L}} : \mathcal{U}_\infty \longrightarrow \Lambda(\mathcal{G})$$

by

$$\widetilde{\mathcal{L}}(\mathbf{u}) = \widetilde{\mathcal{M}}^{-1}(\mathcal{L}(f_{\mathbf{u}}))$$

where $f_{\mathbf{u}}$ denotes the Coleman power series of $\mathbf{u}$ (theorem 5.10) and $\mathcal{L}$ is the same as in lemma 5.14. This is a $\mathcal{G}$-homomorphism, and

$$\mathcal{L}(f_{\mathbf{u}}) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}} \binom{\chi(g)}{n} d\mathcal{L}(\mathbf{u}).$$

The following theorem gives us the exact sequence that we were looking for:

THEOREM 5.26. *We have an exact sequence of $\mathcal{G}$-modules*

$$0 \longrightarrow \mu_{p-1} \times T_p(\mu) \longrightarrow \mathcal{U}_\infty \xrightarrow{\widetilde{\mathcal{L}}} \Lambda(\mathcal{G}) \xrightarrow{\beta} T_p(\mu) \longrightarrow 0,$$

*where the kernel on the left is the natural inclusion and map $\beta$ on the right is given by $\beta(\lambda) = (\zeta_n)^{\int_{\mathcal{G}} \chi \, d\lambda}$.*

Theorem 5.26 essentially follows from the commutative diagram (5.5) seen in section 1, which we now reinterpret via the Coleman power series. Indeed, we have the following commutative diagram, where $\kappa : \mu_{p-1} \times T_p(\mu) \longrightarrow A$ is defined as $\kappa(\zeta, (\zeta_n)^a) = \zeta(1+T)^a$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mu_{p-1} \times T_p(\mu) & \longrightarrow & \mathcal{U}_\infty & \xrightarrow{\widetilde{\mathcal{L}}} & \Lambda(\mathcal{G}) & \xrightarrow{\beta} & T_p(\mu) \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \mathbf{u} \mapsto f_{\mathbf{u}}(T)} & & \downarrow{\scriptstyle \widetilde{\mathcal{M}}} & & \downarrow{\scriptstyle (\zeta_n)^a \mapsto a} \\
0 & \longrightarrow & A & \longrightarrow & W & \xrightarrow{\mathcal{L}} & \Lambda^{\psi=0} & \xrightarrow{\alpha} & \mathbb{Z}_p \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \zeta(1+T)^a \mapsto a} & & \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle \mathrm{id}} \\
0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \Lambda^{\psi=1} & \xrightarrow{\theta} & \Lambda^{\psi=0} & \longrightarrow & \mathbb{Z}_p \longrightarrow 0
\end{array} \tag{5.18}$$

## 4. The $p$-adic zeta function

This section is devoted to the proof of theorem 4.6, i.e., to the proof of the existence of a $p$-adic analogue of the Riemann zeta function. Recall that the (complex) Riemann zeta function is the analytic function which coincides with the Dirichlet series

$$\boldsymbol{\zeta}(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

on the half-plane $\mathrm{Re}(s) > 1$.
It was already know to Euler (at least up to $k = 13$) that for a natural number $k$

$$\boldsymbol{\zeta}(1-2k) = -\frac{\mathcal{B}_{2k}}{2k} \tag{5.19}$$

where $\mathcal{B}_k \in \mathbb{Q}$ is the $k$-th Bernouilli number, defined by

$$\frac{1}{e^t - 1} = \sum_{n=0}^{\infty} \frac{\mathcal{B}_n}{n!} \cdot t^{n-1}. \tag{5.20}$$

$\boldsymbol{\zeta}$ takes the value 0 at even negative integers. By a $p$-adic analogue of the Riemann zeta function, we mean an element of the fraction field of $\Lambda$, which is almost a power series (i.e., a pseudo-measure) which interpolates $\boldsymbol{\zeta}$ at the negative integers.

We will first prove two propositions that we will need to complete the proof of the theorem. We start by introducing the logarithmic derivative homomorphism of elements of $\mathcal{U}_\infty$:

Definition 5.27 (Logarithmic derivative homomorphism). *For each integer $k \geq 1$, define the* logarithmic derivative homomorphism $\delta_k : \mathcal{U}_\infty \longrightarrow \mathbb{Z}_p$ *by*

$$\delta_k(\mathbf{u}) = \left( D^{k-1} \left( \frac{(1+T) f_{\mathbf{u}}(T)}{f_{\mathbf{u}}(T)} \right) \right)_{T=0}$$

*where $\mathbf{u}$ is any element of $\mathcal{U}_\infty$ and $f_{\mathbf{u}}(T)$ is the associated power series of theorem 5.10. The subscript $T = 0$ means evaluation at 0.*

It is worth to notice that $\delta_k$ takes values in $\mathbb{Z}_p$ because $f_{\mathbf{u}}$ is a unit in $\Lambda$. We also recall that $\mathcal{G}$ acts on $\mathcal{U}_\infty$ in the natural fashion and on $\Lambda$ by lemma 5.1. We have the following lemma regarding the logarithmic derivative homomorphism:

Lemma 5.28. *For all $k \geq 1$, the map $\delta_k$ is a group homomorphism satisfying*

$$\delta_k(\sigma(\mathbf{u})) = \chi(\sigma)^k \delta_k(\mathbf{u})$$

*for all $\mathbf{u}$ in $\mathcal{U}_\infty$ and all $\sigma$ in $\mathcal{G}$.*

*Proof.* It is clear that it is a group homomorphism. To see the equality, observe that

$$f_{\sigma(\mathbf{u})}(T) = f_{\mathbf{u}}((1+T)^{\chi(\sigma)} - 1),$$

and apply the identity, which holds for all $k \geq 0$, $a$ in $\mathbb{Z}_p$ and $g$ in $\Lambda$ :

$$D^k(g((1+T)^a - 1)) = a^k (D^k g)((1+T)^a - 1). \tag{5.21}$$

□

We now recall the particular case of example 5.11: let $a$ and $b$ be integers that are prime to $p$ and define $\mathbf{c}(a,b) = (c_n(a,b)) \in \mathcal{U}_\infty$ by

$$c_n(a,b) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}.$$

The computation of its logarithmic derivatives will be useful later on:

Proposition 5.29. *Let $k \geq 1$ be an integer. Then $\delta_k(\mathbf{c}(a,b)) = 0$ for odd $k$ and $\delta_k(\mathbf{c}(a,b)) = (b^k - a^k)\boldsymbol{\zeta}(1-k)$ for even $k$.*

*Proof.* Let

$$f(T) = \frac{(1+T)^{-a/2} - (1+T)^{a/2}}{(1+T)^{-b/2} - (1+T)^{b/2}}$$

so that $f(\pi_n) = c_n(a,b)$ for all $n \geq 0$. Consider the change of variable $T = e^z - 1$ so that $D = d/dz$. We have

$$\delta_k(\mathbf{c}(a,b)) = \left( \left( \frac{d}{dz} \right)^{k-1} g(z) \right)_{z=0}$$

where

$$g(z) = \frac{d}{dz} \log f(e^z - 1).$$

This yields

$$2g(z) = b\left( \frac{1}{e^{-bz}-1} - \frac{1}{e^{bz}-1} \right) - a\left( \frac{1}{e^{-az}-1} - \frac{1}{e^{az}-1} \right).$$

We now recall the definition of Bernouilli numbers (5.20), and since $\mathcal{B}_{2m+1} = 0$ for $m > 0$, we obtain that

$$g(z) = \sum_{k=1}^{\infty} \frac{\mathcal{B}_{2k}}{(2k)!} z^{2k-1}(a^{2k} - b^{2k}).$$

The proposition now follows from (5.19). □

We also have the following theorem regarding the relation of the logarithmic derivative with certain integrals:

PROPOSITION 5.30. *For all $k \geq 1$, and all $\mathbf{u}$ in $\mathcal{U}_\infty$, we have*

$$\int_{\mathcal{G}} \chi(g)^k \, d\widetilde{\mathcal{L}}(\mathbf{u}) = (1 - p^{k-1})\delta_k(\mathbf{u})$$

*where $\delta_k$ is the logarithmic derivative homomorphism.*

*Proof.* We start the proof by noting that for any $\lambda$ in $\Lambda(\mathcal{G})$, the canonical isomorphism $\tilde{\chi}$ given by (5.16) gives

$$\int_{\mathcal{G}} \chi(g)^k \, d\lambda = \int_{\mathbb{Z}_p^\times} x^k \, d(\tilde{\chi}(\lambda)).$$

Also, via our identification of $\Lambda(\mathbb{Z}_p^\times)$ with a subset of $\Lambda(\mathbb{Z}_p)$, the integral on the right hand side has the same value if we integrate over the whole of $\mathbb{Z}_p$. Now take $\lambda = \widetilde{\mathcal{L}}(\mathbf{u})$, so that, by definition, we have $\tilde{\chi}(\widetilde{\mathcal{L}}(\mathbf{u})) = \Upsilon(\mathcal{L}(f_\mathbf{u})$, where we recall that

$$\mathcal{L}(f_\mathbf{u})(T) = \frac{1}{p} \log \left( \frac{f_\mathbf{u}(T)^p}{\varphi(f)(T)} \right).$$

Thus, by lemma 5.23, we have

$$\int_{\mathcal{G}} \chi(g)^k \, d\widetilde{\mathcal{L}}(\mathbf{u}) = \left( D^{k-1}(h_\mathbf{u}(T) - \varphi(h_\mathbf{u})(T)) \right)_{T=0}$$

where

$$h_\mathbf{u}(T) = (1+T)\frac{f'_\mathbf{u}(T)}{f_\mathbf{u}(T)}.$$

We can now apply the identity (5.21) to get the result of the statement. □

Now that we have proved propositions 5.29 and 5.30, we can move towards the proof of theorem 4.6 (the existence of a $p$-adic analogue of the Riemann zeta function). We start the proof with a lemma:

LEMMA 5.31. *Assume that $\lambda$ is any element of $\Lambda(\mathcal{G})$ such that $\chi^k(\lambda) = 0$ for all $k > 0$. Then $\lambda = 0$. The analogous assertion is also valid for pseudo-measures on $\mathcal{G}$.*

*Proof.* Recall the isomorphism (5.17)

$$\widetilde{\mathcal{M}} : \Lambda(\mathcal{G}) \cong \Lambda^{\psi=0}$$

arising from Mathler's theorem. Hence

$$\widetilde{\mathcal{M}}(\lambda) = g(T),$$

where

$$g(T) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}} \binom{\chi(g)}{n} d\lambda.$$

When $n > 0$, the binomial coefficient $\binom{x}{n}$ is a polynomial in $x$ with constant term equal to zero. Therefore, by the hypothesis of the lemma, we have

$$\int_{\mathcal{G}} \binom{\chi(g)}{n} d\lambda = 0 \text{ for } n > 0.$$

Thus $g(T)$ is a constant and must be identically zero since it belongs to $\Lambda^{\psi=0}$. This completes the proof for elements of $\Lambda(\mathcal{G})$.
A consequence of this fact is that if $\lambda$ is any element of $\Lambda(\mathcal{G})$ such that $\chi^k(\lambda) \neq 0$ for all $k > 0$, then $\lambda$ is not a zero divisor. Indeed, if $\lambda \cdot \lambda' = 0$ and $\chi^k$ is a ring homomorphism of $\Lambda(\mathcal{G})$, it follows that $\chi^k(\lambda') = 0$ for all $k > 0$, which implies $\lambda' = 0$.
Now let $\chi$ be a pseudo-measure on $\mathcal{G}$ with $\chi^k(\xi) = 0$ for all $k > 0$. For each $u \in \mathbb{Z}_p^\times$, let $\sigma_u$ denote the unique element of $\mathcal{G}$ with $\chi(\sigma_u) = u$. Now choose $u = 1 + p$. Then

$$\chi^k(\sigma_u - 1) = (1 + p)^k - 1 \neq 0$$

for all $k > 0$. But by hypothesis

$$\chi^k((\sigma_u - 1)\xi) = 0$$

for all $k > 0$, and as $\sigma_u - 1$ is not a zero divisor the previous paragraph tells us that $\xi = 0$. □

Let $Q(\mathcal{G})$ be the total ring of quotients of the Iwasawa algebra $\Lambda(\mathcal{G})$. If one proceeds in the same way as we did at the start of this section, it is clear that we have a decomposition

$$Q(\mathcal{G}) = Q(\mathcal{G})^+ \oplus Q(\mathcal{G})^-$$

and that we can identify pseudo-measures on $G$ with pseudo-measures on $\mathcal{G}$ which lie in $Q(\mathcal{G})^+$.

COROLLARY 5.32. *Let $\lambda$ be an element of $\Lambda(\mathcal{G})$. If $\int_{\mathcal{G}} \chi^k \, d\lambda = 0$ for $k = 1, 3, 5 \ldots$ then $\lambda \in \Lambda(\mathcal{G})^+$, and if $\int_{\mathcal{G}} \chi^k \, d\lambda = 0$ for $k = 2, 4, 6 \ldots$ then $\lambda \in \Lambda(\mathcal{G})^-$. The analogous assertion holds for pseudo-measures on $\mathcal{G}$.*

*Proof.* Assume that $\lambda$ is in $\Lambda(\mathcal{G})$ and let $\lambda = \lambda^+ + \lambda^-$ be its decomposition as in (5.23). Since $\chi(j) = -1$, we have that $\chi^k(1+j) = 0$ for all odd integers $k$ and that $\chi^k(1+j) = 0$ for all even integers $k$. The result follows after applying lemma 5.31. The argument for pseudo-measures is analogous. □

We now present the key ingredient of the proof of the existence of the $p$-adic analogue of the Riemann zeta function.

PROPOSITION 5.33. *There exists a unique pseudo-measure $\tilde{\boldsymbol{\zeta}}_p$ on $\mathcal{G}$ such that*

$$\int_{\mathcal{G}} \chi(g)^k \, d\tilde{\boldsymbol{\zeta}}_p = \begin{cases} (1-p^{k-1})\boldsymbol{\zeta}(1-k) & \text{if } k = 2, 4, \dots \\ 0 & \text{if } k = 1, 3, \dots . \end{cases}$$

Before proving the proposition, we introduce a lemma that will help us prove that $\tilde{\boldsymbol{\zeta}}_p$ is indeed a pseudo-measure.

LEMMA 5.34. *Let $e$ be a primitive root modulo $p$ such that $e^{p-1} \not\equiv 1 \pmod{p^2}$. Let $I(\mathcal{G})$ be the augmentation ideal of $\Lambda(\mathcal{G})$. Then*

$$I(\mathcal{G}) = (\sigma_e - 1)\Lambda(\mathcal{G}) = \Lambda(\mathcal{G})c_n(e, 1),$$

*where $\sigma_u$ is the unique element of $\mathcal{G}$ such that $\chi(\sigma_u) = u$ for each $u \in \mathbb{Z}_p^\times$.*

*Proof.* We just need to notice that $\sigma_e$ is a topological generator of $\mathcal{G}$, and that if $K$ is any finite cyclic group, the augmentation ideal of $\mathbb{Z}_p[K]$ is $(\tau - 1)\mathbb{Z}_p[K]$ where $\tau$ is any generator of $K$. □

*Proof of proposition 5.33.*
The uniqueness is a consequence of the previous lemmas. The hard part of the proof is existence. Let $a$ and $b$ be integers that are prime to $p$ such that $b^2 \neq a^2$. Consider again $\mathbf{c}(a, b) = (c_n(a, b))$ where

$$c_n(a, b) = \frac{\zeta_n^{-a/2} - \zeta_n^{a/2}}{\zeta_n^{-b/2} - \zeta_n^{b/2}}.$$

Now $\mathbf{c}(a, b)$ is in $\mathcal{U}_\infty$. Define $\lambda(a, b)$ in the Iwasawa algebra $\Lambda(\mathcal{G})$ by

$$\lambda(a, b) = \widetilde{\mathcal{L}}(\mathbf{c}(a, b)).$$

We now apply propositions 5.29 and 5.30 to get

$$\int_{\mathcal{G}} \chi(g)^k \, d\lambda(a, b) = \begin{cases} (b^k - a^k)(1-p^{k-1})\boldsymbol{\zeta}(1-k) & \text{if } k = 2, 4, \dots \\ 0 & \text{if } k = 1, 3, \dots . \end{cases} \tag{5.22}$$

Define the element $\theta(a, b) = \sigma_a - \sigma_b$ of $\Lambda(\mathcal{G})$ where the $\sigma_u$ are defined as in lemma 5.34. We thus have that for each integer $k > 0$

$$\chi^k(\theta(a, b)) = b^k - a^k \neq 0$$

because $b^2 \neq a^2$. Hence $\theta(a, b)$ is not a zero divisor in $\Lambda(\mathcal{G})$, so

$$\widetilde{\boldsymbol{\zeta}}_p = \frac{\lambda(a, b)}{\theta(a, b)}$$

lies in $Q(\mathcal{G})$. We now claim that $\widetilde{\boldsymbol{\zeta}}_p$ is independent from the choice of the pair $(a,b)$. Let $(a',b')$ be another choice. By (5.22) we have

$$\chi^k(\theta(a',b')\lambda(a,b)) = \chi^k(\theta(a,b)\lambda(a',b'))$$

for all integers $k>0$. We now apply 5.31 to get

$$\theta(a',b')\lambda(a,b) = \theta(a,b)\lambda(a',b')$$

which establishes the independence of $\widetilde{\boldsymbol{\zeta}}_p$ of the choice of $(a,b)$.

We finally want to prove that $\widetilde{\boldsymbol{\zeta}}_p$ is indeed a pseudo-measure. Take $a=e$, $b=1$ where $e^{p-1}\not\equiv 1 \pmod{p^2}$. By lemma 5.34 the augmentation ideal $I(\mathcal{G})$ of $\Lambda(\mathcal{G})$ is generated by $\theta(e,1)$. But if $\sigma$ is any element of $\mathcal{G}$, then $\sigma-1$ belongs to $I(\mathcal{G})$ and therefore $\sigma-1=\theta(e,1)\lambda$ for some $\lambda$ in $\Lambda(\mathcal{G})$. This proves that $(\sigma-1)\widetilde{\boldsymbol{\zeta}}_p$ belongs to $\Lambda(\mathcal{G})$ as required. □

We proved the existence of a pseudo-measure over $\mathcal{G}=\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$, but we formulated Iwasawa's theorem in terms of the group $G=\mathrm{Gal}(F_\infty/\mathbb{Q})$, so we will to work a bit more to show that we can identify the Iwasawa algebra $\Lambda(G)$ with a sub-algebra of $\Lambda(\mathcal{G})$. Let

$$\mathcal{J}=\mathrm{Gal}(\mathcal{F}_\infty/F_\infty)=\{1,j\}.$$

If $M$ is any $\mathbb{Z}_p[\mathcal{J}]$-module, since $p$ is odd, we have the decomposition

$$M=M^+\oplus M^-,\ \text{where } M^+=\frac{1+j}{2}M \text{ and } M^-=\frac{1-j}{2}M.$$

Since $\Lambda(\mathcal{G})$ is a $\mathbb{Z}_p[\mathcal{J}]$-module, we have

$$\Lambda(\mathcal{G})=\Lambda(\mathcal{G})^+\oplus\Lambda(\mathcal{G})^-. \tag{5.23}$$

Lemma 5.35. *The restriction to $\Lambda(\mathcal{G})^+$ of the natural surjection from $\Lambda(\mathcal{G})$ onto $\Lambda(G)$ induces an isomorphism*

$$\Lambda(\mathcal{G})^+\cong\Lambda(G).$$

*Proof.* Recall that

$$\mathcal{F}_n=\mathbb{Q}(\mu_{p^{n+1}}),\quad F_n=\mathbb{Q}(\mu_{p^{n+1}})^+,$$

and write $\mathcal{G}_n=\mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$, $G_n=\mathrm{Gal}(F_n/\mathbb{Q})$. Let

$$\pi_n:\mathbb{Z}_p[\mathcal{G}_n]\longrightarrow\mathbb{Z}_p[G_n]$$

denote the natural surjection We claim that $\pi_n$ induces an isomorphism from $\mathbb{Z}_p[\mathcal{G}_n]^+$ onto $\mathbb{Z}_p[G_n]$. Indeed, it is clear that $\pi_n$ is surjective, and that it maps $\mathbb{Z}_p[\mathcal{G}_n]^-$ to zero. It can also be shown using eigenspaces decomposition that the $\mathbb{Z}_p$-rank of $\mathbb{Z}_p[\mathcal{G}_n]^+$ is equal to $((p-1)/2)p^n$. The assertion of the lemma follows on passing to the projective limit. □

Thanks to this lemma, from now on we shall identify $\Lambda(G)$ with the subalgebra $\Lambda(\mathcal{G})^+$ of $\Lambda(\mathcal{G})$.

Theorem 4.6 is a direct consequence of corollary 5.32, proposition 5.33 and the identification of lemma 5.35. We reproduce it here again for convenience of the reader.

THEOREM ($p$-adic analogue of the Riemann zeta function). *There exists a unique pseudo-measure $\boldsymbol{\zeta}_p$ on $G$ such that*

$$\int_G \chi(g)^k \, \mathrm{d}\boldsymbol{\zeta}_p = (1 - p^{k-1})\boldsymbol{\zeta}(1-k)$$

*for all even integers $k \geq 2$, where $\chi$ is the cyclotomic character and $\boldsymbol{\zeta}$ is the Riemann zeta function.*

The pseudo-measure $\boldsymbol{\zeta}_p$ is, of course, the desired $p$-adic analogue of the Riemann zeta function. □

## 5. Iwasawa's theorem

We will end this thesis with the proof of the Iwasawa theorem (theorem 4.8). It should be noted that, although we presented it after stating the Iwasawa Main Conjecture, it was proved before the IMC was conjectured, and in fact its proof led to the discovery of the IMC. The original proof by Iwasawa can be found in [**6**] and is very different from the one that we give here.

We will now proceed to repeat and expand a bit the notions about cyclotomic units that we discussed before introducing theorem 4.8 in the previous chapter. A detailed treatment of this theory can be found in [**6**] and [**15**]. Recall that, as in the beginning of the chapter, we denote $\pi_n = \zeta_n - 1$.

For each $n \geq 0$, we define $\mathcal{D}_n$ to be the intersection of the group of global units of $\mathcal{F}_n$ with the subgroup of $\mathcal{F}_n^\times$ generated by the $\sigma(\pi_n)$ where $\sigma$ runs over the elements of $\mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$. We also define $D_n = \mathcal{D}_n \cap F_n$. It is well known that $D_n$ is generated by all the Galois conjugates of $\pm c_n(e,1)$, where

$$c_n(e,1) = \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}},$$

and the integer $e$ is a primitive root modulo $p$ and $e^{p-1} \not\equiv 1 \pmod{p^2}$. It is a classical result that $D_n$ has finite index in the group of all units of $F_n$, and that this index is equal to the class number of $F_n$. We defined the local fields

$$\mathcal{K}_n = \mathbb{Q}_p(\mu_{p^{n+1}}), \; K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+.$$

If $A$ is any subset of these fields, then we will denote by $\overline{A}$ its closure in the $p$-adic topology. Now we introduce

$$\mathcal{C}_n = \overline{\mathcal{D}_n}, \; C_n = \overline{D_n}.$$

Recall that earlier in this chapter we defined $\mathcal{U}_n$ to be the group of units of $\mathcal{K}_n$. We will denote by $\mathfrak{p}_n$ the maximal ideal of the ring of integers of $\mathcal{K}_n$. In a similar fashion, we will denote by $U_n$ the group of units of $K_n$, and by $\mathcal{U}_n^1$ the subgroup $\{x \in \mathcal{U}_n | x \equiv 1 \pmod{\mathfrak{p}_n}$. If $Z$ is any subgroup of $\mathcal{U}_n$, we write $Z^1 = Z \cap \mathcal{U}_n^1$. It is worth to notice that the index of $Z^1$ in $Z$ always divides $p-1$, because $Z^1$ is the kernel of the reduction map from $Z$ to $\mathbb{F}_p^\times$.

This means that this index is prime to $p$. We can also note that $\mathcal{U}_n^1$ and $U_n^1$ are $\mathbb{Z}_p$-modules, but $\mathcal{U}_n$ and $U_n$ are not.
We are interested in the groups $C_n^1$ and $U_n^1$ and their projective limits

$$U_\infty^1 = \lim_{\leftarrow} U_n^1,\ C_\infty^1 = \lim_{\leftarrow} C_n^1,$$

where we take the limits with respect to the norm maps. Since $U_n^1$ and $C_n^1$ are compact $\mathbb{Z}_p$-modules, so are $U_\infty^1$ and $C_\infty^1$. Further, they are endowed a with natural continuous action of $G$. Therefore they become modules over the Iwasawa algebra $\Lambda(G)$. We take $e$ as before, i.e., $e$ is a primitive root modulo $p$ and $e^{p-1} \not\equiv 1 \pmod{p^2}$. We will need the following lemma in the final steps of the proof of the Iwasawa theorem.

LEMMA 5.36. *We have $C_\infty^1 = \Lambda(G)\mathbf{b}$ where $\mathbf{b} = (b_n)$ is given by*

$$b_n = uc_n(e,1) \text{ for } n \geq 0,$$

*and $u$ is the unique $(p-1)$-th root of unity in $\mathbb{Q}_p$ such that $eu \equiv 1 \pmod{p}$.*

*Proof.* Since $u^p = u$, it is clear that $\mathbf{b} = (b_n)$ belongs to $U_\infty$. Moreover, we claim that $b_n \equiv 1 \pmod{\mathfrak{p}_n}$ for all $n \geq 0$. Indeed, if $f_{\mathbf{c}}(T)$ is the Coleman power series of $\mathbf{c} = (c_n(e,1))$, then $f_{\mathbf{c}}(0) = e$, as follows from the explicit description given in example 5.11. Hence $c_n(e,1) \equiv e \pmod{\mathfrak{p}_n}$ and our assertion is clear.
We also need to show that $b_n$ lies in the closure of $D_n^1$, but it is clear because $b_n^{p-1}$ lies in $D_n^1$ and $p-1$ is a $p$-adic unit. Now put $\mathfrak{b} = \Lambda(G)\mathbf{b}$ and let $h_n : C_\infty^1 \longrightarrow C_n^1$ be the natural projection. To show that $\mathfrak{b} = C_\infty^1$, it suffices to prove that

$$h_n(\mathfrak{b}) = C_n^1 \text{ for all } n \geq 0.$$

But $h_n(\mathfrak{b})$ is clearly the $\mathbb{Z}_p$-submodule generated by the $\sigma(b_n)$ for all $\sigma$ in $\mathrm{Gal}(F_n/\mathbb{Q})$. The assertion now follows from the fact that the $\pm\sigma(c_n(e,1))$ generate $D_n$ as a $\mathbb{Z}$-module. □

We are now ready to prove theorem 4.8, which we reproduce here for convenience of the reader.

THEOREM. *The $\Lambda(G)$-module $U_\infty^1/C_\infty^1$ is canonically isomorphic to $\Lambda(G)/I(G)\boldsymbol{\zeta}_p$ where $\boldsymbol{\zeta}_p$ is the $p$-adic zeta function, and $I(G)$ is the augmentation ideal.*

*Proof.* Note that, since the norm map from $K_n$ to $K_{n-1}$ induces the identity map on the residue fields, we have

$$\mathcal{U}_\infty = \mu_{p-1} \times \mathcal{U}_\infty^1,\ U_\infty = \mu_{p-1} \times U_\infty^1.$$

We may now rewrite the fundamental exact sequence of theorem 5.26 as

$$0 \longrightarrow T_p(\mu) \longrightarrow \mathcal{U}_\infty^1 \xrightarrow{\mathcal{L}^1} \Lambda(\mathcal{G}) \longrightarrow T_p(\mu) \longrightarrow 0,$$

where we define $\mathcal{L}^1$ as the restriction of $\widetilde{\mathcal{L}}$ to $\mathcal{U}_\infty^1$. Since $p$ is odd, the exact sequence remains exact after taking invariants under $\mathcal{J} = \{1, j\}$. But since $T_p(\mu)^{\mathcal{J}} = 0$, we get a canonical isomorphism

$$\mathcal{L}^1 : U_\infty^1 \cong \Lambda(G).$$

But lemma 5.36 gives

$$C_\infty^1 = \Lambda(G)\mathbf{b},$$

so we get

$$\mathcal{L}^1(C^1_\infty) = \Lambda(G)\mathcal{L}^1(\mathbf{b}).$$

We now recall the proof of proposition 5.33 to get $\mathcal{L}^1(\mathbf{b}) = \boldsymbol{\zeta}_p\theta^+(e,1)$ where $\theta^+(e,1)$ denotes the image of $\theta(e,1)$ in $\Lambda(G)$. Now if we consider the analogue of lemma 5.34 for $G$ we get $\Lambda(G)\theta^+(e,1) = I(G)$. This completes the proof of the theorem. □

# References


[1] N. Bourbaki, *Elements of Mathematics, Commutative Algebra*, Springer (1989).

[2] J. Coates, R. Sujatha. *Cyclotomic Fields and Zeta Values*, Springer Monographs in Mathematics, Springer (2006).

[3] R. Coleman, *Division values in local fields*, Invent. Math. **53** (1979), 91-116.

[4] R. Greenberg, *On the Iwasawa Invariants of Totally Real Number Fields*, Amer. J. Math. **98** (1976), 263-284.

[5] K. Iwasawa, *On* $\Gamma$*-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183-226.

[6] K. Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **20** (1964), 42-82.

[7] K. Iwasawa, *On p-adic L-functions*, Ann. of Math. **89** (1969), 198-205.

[8] V. Kolyvagin, *Euler systems*, in The Grothendieck Festschrift, Vol. II, Progr. Math. **87**, Birkhuser Boston, Boston, MA (1990), 435 - 483.

[9] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*, Crelle J., **199** (1958), 23-34.

[10] B. Mazur, A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179-330.

[11] J.S. Milne, *Algebraic Number Theory* (v3.02), available at www.jmilne.org/math (2009).

[12] K. Rubin, appendix, in S. Lang, *Cyclotomic fields I and II, Combined second edition*, Graduate Texts In Mathematics **121**, Springer (1990).

[13] J.P. Serre, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki Exp. no. **174**, (1958).

[14] R. Sharifi, *Iwasawa Theory*. Online notes, available at http://math.ucla.edu/~sharifi/iwasawa.pdf [last checked the 14th of September, 2018].

[15] W. Sinott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. of Math. **108** (1978), 107-134.

[16] C. Skinner, E. Urban, *The Iwasawa main conjectures for* $\mathrm{GL}_2$, Invent. Math. **195.1** (2014), 1-277.

[17] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. **128** (1988), 1-18.

[18] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer (1982).